Benutzerhandbuch - Deutsch

FUJITSU

FUJITSU Software ServerView Suite

Remote Management

iRMC S2/S3 - integrated Remote Management Controller

Ausgabe Juli 2012

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2000

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2000 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Copyright © 2012 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.
Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhalt

1 Einleitung 11

1.1 Zielgruppen und Zielsetzung des Handbuchs 12
1.2 Funktionen des iRMC S2/S3 (Überblick) 13
1.3 Kommunikationsschnittstellen des iRMC S2/S3 20
1.4 Kommunikationsprotokolle, die vom iRMC S2/S3 genutzt werden 21
1.5 IPMI - Technischer Hintergrund 22
1.6 DCMI (Data Center Management Interface) 30
1.7 Änderungen gegenüber den vorherigen Ausgaben 31
1.8 ServerView Suite Link-Sammlung 35
1.9 Dokumentation zur ServerView Suite 36
1.10 Darstellungsmittel 37

2 Zum ersten Mal am iRMC S2/S3 anmelden 39

2.1 Voraussetzungen 39
2.2 iRMC S2/S3-Voreinstellungen 40
2.3 An der iRMC S2/S3-Web-Oberfläche anmelden 41

3 iRMC S2/S3 konfigurieren 43

3.1 LAN-Schnittstelle des iRMC S2/S3 konfigurieren 43
3.1.1 Voraussetzungen 44
3.1.1.1 An der richtigen LAN-Schnittstelle gesteckt? 44
3.1.1.2 Zusammenspiel der IP-Adressen des iRMC S2/S3 und des Systems 45
3.1.1.3 Zugriff aus einem anderen Sub-Netz 45
3.1.2 LAN-Schnittstelle konfigurieren: Konfigurationstools 45
3.1.3 LAN-Schnittstelle des iRMC S2/S3 mit dem BIOS / TrustedCore / UEFI Setup Utility konfigurieren 46

3.1.3.1 LAN-Schnittstelle des iRMC S2 über das BIOS / TrustedCore Setup Utility konfigurieren . . . 46
3.1.3.2 LAN-Schnittstelle des iRMC S3 über das UEFI Setup Utility konfigurieren . . . 48
3.1.4 LAN-Schnittstelle testen . . . 49

3.2 Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren . . . 50
3.2.1 Text-Konsolen-Umleitung für den iRMC S2 konfigurieren . . . 51
3.2.2 Text-Konsolen-Umleitung für den iRMC S3 konfigurieren . . . 55
3.2.3 Konsolen-Umleitung bei laufendem Betriebssystem nutzen . . . 57

3.3 Serielle Schnittstelle des iRMC S2/S3 konfigurieren und nutzen . . . 59
3.3.1 Die serielle Schnittstelle des iRMC S2 konfigurieren . . . 60
3.3.2 Die serielle Schnittstelle des iRMC S3 konfigurieren . . . 62
3.3.3 Benutzeroberfläche Remote Manager (Serial) nutzen . . . 65

3.4 iRMC S2/S3 über die iRMC S2/S3-Web-Oberfläche konfigurieren . . . 66
3.4.1 LAN-Parameter konfigurieren . . . 66
3.4.2 Alarmbenachrichtigung (Alerting) konfigurieren . . . 67
3.4.3 Text-Konsolen-Umleitung konfigurieren . . . 67

4 Benutzerverwaltung für den iRMC S2/S3 . . . 69

4.1 Konzept der Benutzerverwaltung für den iRMC S2/S3 . . . 70

4.2 Benutzerberechtigungen . . . 72

4.3 Lokale Benutzerverwaltung für den iRMC S2/S3 . . . 74
4.3.1 Lokale Benutzerverwaltung über die iRMC S2/S3-Web-Oberfläche . . . 74
4.3.2 Lokale Benutzerverwaltung über den Server Configuration Manager . . . 75
4.3.3 SSHv2 Public Key-Authentifizierung für lokale iRMC S2/S3-Benutzer . . . 76
4.3.3.1 Öffentlichen und privaten SSHv2-Schlüssel erzeugen . . . 78
4.3.3.2 Öffentlichen SSHv2-Schlüssel aus Datei auf den iRMC S2/S3 laden. . . . 82
4.3.3.3 PuTTY und OpenSSH Client für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren . . . 84
4.3.3.4 Beispiel: Öffentlicher SSHv2-Schlüssel . . . 90

5 Grafische Konsolen-Umleitung (AVR) 91

5.1 Voraussetzungen: Die Einstellungen für die AVR überprüfen 92

5.2 AVR verwenden 94
5.2.1 Geringe Bandbreite verwenden 96
5.2.2 Parallele AVR-Sitzungen 96
5.2.3 „Lokaler Bildschirm Aus“-Funktionalität 97
5.2.4 Umleitung der Tastatur 98
5.2.5 Umleitung der Maus 100
5.2.5.1 Mauszeiger synchronisieren 100
5.2.5.2 Verwalteter Windows Server: Einstellungen für Mauszeiger-Synchronisation anpassen 102
5.2.5.3 Verwalteter Linux Server: Einstellungen für Mauszeiger-Synchronisation anpassen 105

5.3 Menüs des AVR-Fensters 108
5.3.1 Menü Extras 109
5.3.2 Menü Remote Storage 112
5.3.3 Menü Ein-/Ausschalten 113
5.3.4 Menü Sprachen 114
5.3.5 Menü Präferenzen 115

6 Remote Storage 117

6.1 Remote Storage am Remote-Arbeitsplatz bereitstellen . . . 119
6.1.1 Remote Storage starten 120
6.1.2 Speichermedien für Remote Storage bereitstellen 123
6.1.3 Speichermedien als Remote Storage verbinden 127
6.1.4 Remote Storage-Verbindungen trennen 131
6.1.5 Speichermedien entfernen 132

6.2 Remote Storage via Remote Storage Server bereitstellen . 133
6.2.1 Remote Storage Server installieren 134
6.2.2 Ausführungsmodi des Remote Storage Servers 135
6.2.3 Remote Storage Server konfigurieren, starten und beenden . . 136

7 iRMC S2/S3-Web-Oberfläche 141

7.1 An der iRMC S2/S3-Web-Oberfläche anmelden 142

7.2 Erforderliche Benutzerberechtigungen 144

7.3 Aufbau der Bedienoberfläche 149

7.4 System Informationen - Informationen zum Server 152

7.4.1 System Überblick - Allgemeine Informationen zum Server 153

7.4.2 System Komponenten Information - Informationen zu den Server-Komponenten 158

7.5 BIOS-Einstellungen sichern/wiederherstellen, BIOS aktualisieren 161

7.5.1 BIOS-Parameter und -Einstellungen in Datei sichern / aus Datei wiederherstellen 161

7.5.1.1 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format sichern 162

7.5.1.2 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format wiederherstellen 164

7.5.2 BIOS aktualisieren via "Aktualisierung aus Datei" oder via TFTP 166

7.6 iRMC S2/S3 - Informationen, Firmware und Zertifikate . . . 171

7.6.1 iRMC S2/S3 Informationen - Informationen zum iRMC S2/S3 . 172

7.6.2 iRMC S2/S3 Firmware Einstellungen abspeichern 176

7.6.3 Zertifikat Austausch - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden 178

7.6.4 Selbstsigniertes RSA Zertifikat erzeugen 185

7.6.5 iRMC S2/S3 Firmware Aktualisierung 187

7.7 Energieverwaltung 193

7.7.1 Ein-/Ausschalten - Server ein-/ausschalten 194

7.7.2 Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren 198

7.7.3 Netzteil Information - Stromversorgung und IDPROM-Daten der FRU-Komponenten 205

7.8 Energieverbrauch - Energieverbrauch des Servers steuern 206

7.8.1 Konfiguration der Energieverbrauchssteuerung - Energieverbrauch des Servers konfigurieren 207

7.8.2 Aktueller System Energieverbrauch - aktuellen Energieverbrauch anzeigen 213

7.8.3 Energieverbrauch Verlauf - zeitlichen Verlauf des Energieverbrauchs anzeigen 214

7.9 Sensoren - Status der Sensoren überprüfen 218

7.9.1 Lüfter - Lüfter überprüfen 219
7.9.2 Temperatur - Temperatursensoren überprüfen 221
7.9.3 Spannungen - Spannungssensoren überprüfen 223
7.9.4 Netzteil - Stromversorgung überprüfen 224
7.9.5 Komponenten Status - Status der Serverkomponenten überprüfen 226

7.10 Fehlerspeicher und interner Ereignisspeicher 229
7.10.1 IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge 230
7.10.2 Interne Ereignisliste - Information zum internen Ereignisspeicher und Anzeige der Einträge 233
7.10.3 Fehlerspeicher Konfiguration - IPMI SEL und internen Ereignisspeicher konfigurieren 236

7.11 Server Management Informationen - Server-Einstellungen konfigurieren 239

7.12 Netzwerk Einstellungen - LAN-Parameter des iRMC S2/S3 konfigurieren 244
7.12.1 Netzwerk Schnittstelle- Ethernet-Einstellungen des iRMC S2/S3 konfigurieren 245
7.12.2 Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren 252
7.12.3 DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren . . 256

7.13 Benachrichtigungen - Alarmbenachrichtigung konfigurieren 260
7.13.1 SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren 261
7.13.2 Serielle / Modem Benachrichtigungen - Alarmweiterleitung über Modem konfigurieren 263
7.13.3 E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren 265

7.14 Benutzerverwaltung 272
7.14.1 Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S2/S3 272
7.14.1.1 Neuen Benutzer konfigurieren 274
7.14.1.2 Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details) 275
7.14.2 Verzeichnisdienst Konfiguration (LDAP) - Verzeichnisdienst am iRMC S2/S3 konfigurieren 282
7.14.2.1 iRMC S2/S3 für Microsoft Active Directory konfigurieren . . 285

7.14.2.2 iRMC S2/S3 für Novell eDirectory / OpenLDAP / OpenDS konfigurieren 290
7.14.3 Centralized Authentication Service (CAS) Konfiguration - CAS Service konfigurieren 296
7.15 Konsolen-Umleitung 302
7.15.1 BIOS Text Konsole - Text-Konsolen-Umleitung konfigurieren und starten 302
7.15.1.1 BIOS Konsolen Umleitung Optionen - Text-Konsolen-Umleitung konfigurieren 303
7.15.1.2 Text Konsolen Umleitung (via Serial Over LAN) - Text-Konsolen-Umleitung starten 305
7.15.1.3 Text-Konsolen-Umleitung bei laufendem Betriebssystem . . 310
7.15.2 Grafische Konsolen Umleitung (AVR) - Grafische Konsolen-Umleitung (AVR) starten 312
7.16 Remote Storage 323
7.17 iRMC S2/S3 über Telnet / SSH (Remote Manager) bedienen 326

8 iRMC S2/S3 über Telnet/SSH (Remote Manager) 333

8.1 Voraussetzung am verwalteten Server 334
8.2 Remote Manager bedienen 335
8.3 Menü-Übersicht 336
8.4 Anmeldeprozess 338
8.5 Hauptmenü des Remote Manager 340
8.6 Erforderliche Benutzerberechtigungen 342
8.7 Passwort ändern 344
8.8 System Information - Informationen zum verwalteten Server 344
8.9 Power Management 345
8.10 Enclosure Information - System / interner Eventlog, Status der Sensoren 346
8.11 Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S2 350
8.12 Console Redirection (EMS/SAC) - Text-Konsolen-Umleitung starten 351

8.13 Start a Command Line shell... - SMASH CLP Shell starten . 351
8.14 Console Logging - Meldungsausgabe auf die Text-Konsole (seriell) 353
8.15 Command Line Protocol (CLP) 355

9 iRMC S2/S3 via Server Configuration Manager konfigurieren . 359

9.1 Server Configuration Manager via ServerView Installation Manager aufrufen 360
9.2 Server Configuration Manager über das Windows Startmenü aufrufen 360
9.3 Server Configuration Manager über den Operations Manager aufrufen 362

10 Firmware aktualisieren 365

10.1 Firmware des iRMC S2/S3 (Überblick) 366
10.2 USB Memory Stick erstellen 369
10.3 Firmware-Image aktualisieren 372
10.3.1 Update über die iRMC S2/S3-Web-Oberfläche 372
10.3.2 Update via ServerView Update Manager 373
10.3.3 Online-Update via ServerView Update Manager Express oder ASP 374
10.3.4 Update mit den Betriebssystem-Flash-Tools 375
10.3.5 Update über das Menü der FlashDisk 377
10.4 Emergency Flash 380
10.5 Flash-Tools 381

11 Remote-Installation des Betriebssystems via iRMC S2/S3 . 385

11.1 Betriebssystem via iRMC S2/S3 installieren - generelles Vorgehen 386
11.2 Speichermedium als Remote Storage verbinden 388

11.3 Verwalteten Server von der ServerView Suite DVD 1 booten und via Installation Manager konfigurieren 391

11.4 Betriebssystem nach Konfiguration auf dem verwalteten Server installieren 396

11.4.1 Windows nach Konfiguration auf dem verwalteten Server installieren 396

11.4.2 Linux nach Konfiguration auf dem verwalteten Server installieren 399

12 Anhang 403

12.1 Vom iRMC S2/S3 unterstützte IPMI OEM-Kommandos . . . 403

12.1.1 Überblick 403

12.1.2 Beschreibung der IPMI OEM-Kommandos 405

12.1.2.1 Beschreibungsformat 405

12.1.2.2 SCCI-konforme Power On/Off-Kommandos 406

12.1.2.3 SCCI-konforme Kommunikationskommandos 411

12.1.2.4 SCCI-konformes Signalkommando 413

12.1.2.5 Firmware-spezifische Kommandos 414

12.1.2.6 BIOS-spezifische Kommandos 418

12.1.2.7 iRMC S2/S3-spezifische Kommandos 420

12.2 iRMC S2/S3 mit SCCI und per Script-Konfiguration konfigurieren 431

12.2.1 iRMC S2/S3-Konfigurationsdaten 431

12.2.1.1 Überblick 431

12.2.1.2 SCCI-Dateiformat 433

12.2.1.3 Einschränkungen 437

12.2.1.4 Konfigurationsdaten aus/auf iRMC S2/S3 exportieren/importieren 438

12.2.2 Script-Konfiguration des iRMC S2/S3 439

12.2.2.1 Liste der vom iRMC S2/S3 unterstützten SCCI-Kommandos 439

12.2.2.2 Scripte mit cURL 440

12.2.2.3 Scripte mit Visual Basic (VB) Script 441

12.2.2.4 Scripte mit Python 442

12.2.2.5 Verschlüsselte Kennwörter mit dem Programm iRMC_PWD.exe generieren 443

1 Einleitung

Moderne Serversysteme werden zunehmend komplexer. Entsprechend steigen auch die Anforderungen an das Management dieser Systeme.

Als Reaktion auf diese Entwicklung gründeten einige Hersteller die Initiative „Intelligent Platform Management Interface (IPMI)“ mit dem Ziel der Definition einer standardisierten, abstrakten und Mitteilung-basierten Schnittstelle zwischen dem zentralen System-Controller (Baseboard Management Controller - BMC) und intelligenter Hardware zum Plattform-Management. Näheres zu IPMI finden Sie im Abschnitt "IPMI - Technischer Hintergrund" auf Seite 22.

iRMC S2 (**i**ntegrated **R**emote **M**anagement **C**ontroller) und iRMC S3 (im Folgenden kurz iRMC S2/S3) sind BMCs mit integriertem LAN-Anschluss und erweiterter Funktionalität. Auf diese Weise bietet der iRMC S2/S3 die umfassende Kontrolle von PRIMERGY Servern, unabhängig vom Systemstatus. Insbesondere ermöglicht der iRMC S2/S3 das „Out-of-Band“-Management (Lights-out-Management, LOM) von PRIMERGY Servern. Für das Out-of-Band-Management wird ein dedizierten Managementkanal genutzt, über den der Systemadministrator den Server via Fernüberwachung verwalten kann. Dabei spielt es keine Rolle, ob der Server ein- oder ausgeschaltet ist.

Bild 1: iRMC S2 auf der Systembaugruppe eines PRIMERGY Servers

Als autonomes System auf der Systembaugruppe eines aktuellen PRIMERGY Servers verfügt der iRMC S2/S3 über ein eigenes Betriebssystem, einen eigenen Web-Server sowie eine eigene Benutzerverwaltung und ein eigenständiges Alarm-Management. Der iRMC S2/S3 wird auch im Stand-by-Betrieb des Servers mit Strom versorgt.

Im vorliegenden Handbuch werden Konfiguration und Bedienoberflächen des iRMC S2/S3 beschrieben.

1.1 Zielgruppen und Zielsetzung des Handbuchs

Das Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Hard- und Software-Kenntnisse verfügen. Es vermittelt Grundkenntnisse zur IPMI-Technologie und informiert ausführlich über folgende Themen:

- Anmelden am iRMC S2/S3
- Konfiguration des iRMC S2/S3
- Benutzerverwaltung am iRMC S2/S3
- Grafische Konsolen-Umleitung (Advanced Video Redirection) via iRMC S2/S3
- Remote Storage via iRMC S2/S3
- iRMC S2/S3-Web-Oberfläche
- Telnet/SSH-basierte Oberfläche (Remote Manager) des iRMC S2/S3
- Konfiguration des iRMC S2/S3 über den Server Configuration Manager
- Firmware-Aktualisierung
- Remote-Installation des Betriebssystem via iRMC S2/S3
- IPMI OEM-Kommandos

Service

Falls Sie weitere Fragen zum Remote Management für PRIMERGY-Server haben, wenden Sie sich an Ihren zuständigen Service und Supportpartner.

Weitere Informationen

http://www.ts.fujitsu.com

1.2 Funktionen des iRMC S2/S3 (Überblick)

Der iRMC S2/S3 unterstützt eine Vielzahl von standardmäßig angebotenen Funktionen. Mit der grafischer Konsolen-Umleitung (Advanced Video Redirection, AVR) und Remote Storage bietet der iRMC S2/S3 außerdem zwei zusätzliche, fortschrittliche Leistungsmerkmale für das Remote Management von PRIMERGY Servern. Für die Nutzung von AVR und Remote Storage benötigen Sie einen gültigen Lizenzschlüssel (License Key), den Sie käuflich erwerben können.

Standardfunktionalität des iRMC S2/S3

- Browser-Zugang

  Der iRMC S2/S3 verfügt über einen eigenen Web-Server, der von der Management-Station über einen Standard Web-Browser angesprochen werden kann.

- Sicherheit (SSL, SSH)

  Der Zugang zum Web-Server kann, ebenso wie die grafische Konsolen-Umleitung inklusive Maus und Tastatur, über HTTPS/SSL abgesichert werden. Für den Zugriff auf den iRMC S2/S3 über den Remote Manager kann eine kryptografisch gesicherte Verbindung eingerichtet werden, die durch die Mechanismen von SSH abgesichert ist. Der Remote Manager ist eine alphanumerische Bedienoberfläche des iRMC S2/S3.

- ServerView-Integration

  Die ServerView-Agenten erkennen den iRMC S2/S3 und ordnen ihn automatisch dem betreffenden Server zu. Damit lässt sich die iRMC S2/S3-Web-Oberfläche ebenso wie die Textkonsolen-Umleitung über das ServerView Remote Management Frontend direkt aus dem ServerView Operations Manager heraus starten.

- Energieverwaltung (Power Management)

  Unabhängig vom Systemzustand haben Sie folgende Möglichkeiten, vom Remote-Arbeitplatz aus den verwalteten Server ein- und auszuschalten:

  – über die iRMC S2/S3-Web-Oberfläche
  – über den Remote Manager und das Command Line Interface (CLP)
  – per Script

- Steuerung des Energieverbrauchs (Power Consumption Control)

  Der iRMC S2/S3 ermöglicht eine umfassende Energieverbrauchssteuerung am verwalteten Server. Darüber hinaus können Sie den Modus festlegen (minimaler Stromverbrauch oder maximale Performance), nach dem der iRMC S2/S3 den Energieverbrauch am verwalteten Server regelt. Zwischen diesen Modi können Sie beliebig umschalten.

- Customer Self Service (CSS)

  An der iRMC S2/S3-Web-Oberfläche informieren die Übersichtstabellen zu Server-Komponenten, Sensoren und Stromversorgung in einer gesonderten Spalte, ob es sich bei der betreffenden Server-Komponente um eine CSS-Komponente handelt. Ferner zeigt der Fehlerspeicher (System Eventlog, SEL) in der Fehlerliste für jedes Ereignis an, ob das betreffende Ereignis von einer CSS-Komponente ausgelöst wurde.

- Text-Konsolen-Umleitung

  Über das ServerView Remote Management Frontend können Sie eine Telnet/SSH-Sitzung am iRMC S2/S3 starten. Es wird dann der Remote Manager aufgerufen, über den Sie eine Text-Konsolumleitung starten können.

- Grundfunktionen eines BMC

  Der iRMC S2/S3 unterstützt die Grundfunktionen eines BMC wie Spannungsmonitoring, Event-Logging und Recovery-Kontrolle.

- „Headless“ Systembetrieb

  Maus, Bildschirm und Tastatur sind am verwalteten Server nicht erforderlich. Daraus resultieren Vorteile, wie niedrigere Kosten, wesentlich einfachere Verkabelung im Rack und höhere Sicherheit.

- Identifizierungs-LED

  Zur einfacheren Identifizierung eines Systems, z.B. in einem voll ausgebauten Rack, können Sie über die iRMC S2/S3-Web-Oberfläche die Identifizierungs-LED einschalten.

- Fehler-LED (Gobal Error-LED)

  Eine Fehler-LED informiert Sie jederzeit über den Status des verwalteten Systems und liefert zugleich den CSS (Customer Self Service)-Status.

- Power LED

  Die Power-LED informiert Sie, ob der Server zurzeit ein- oder ausgeschaltet ist.

- LAN

  Bei einigen Systemen ist die LAN-Schnittstelle der eingebauten System-Netzkarte (Network Interface Card) des Servers dediziert für das Management LAN reserviert. Bei anderen Systemen können Sie diese LAN-Schnittstelle per Konfiguration wahlweise

  – für das Management LAN reservieren,
  – für den „Shared“-Betrieb mit dem System einrichten oder
  – ganz dem System zur Verfügung stellen.

  Dem iRMC S2/S3 zugeordnet sind die Ports, die mit dem Symbol eines Schraubenschlüssels gekennzeichnet ist (siehe Bild 7 auf Seite 44).

- Command Line Interface (CLP)

  Der iRMC S2/S3 unterstützt neben dem Remote Manager auch das von der DMTF (Distributed Management Task Force) standardisierte SMASH CLP (**S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol)

- Einfache Konfiguration - interaktiv oder skript-basiert

  Für die Konfiguration des iRMC S2/S3 stehen Ihnen folgende Tools zur Auswahl:

  – iRMC S2/S3-Web-Oberfläche
  – Server Configuration Manager
  – Server Management-Tool IPMIVIEW
  – BIOS Setup

  Die Konfiguration via Server Configuration Manager oder IPMIVIEW können Sie auch skript-basiert durchführen. Auf diese Weise kann bei der ersten Konfiguration des Servers mit dem ServerView Installation Manager auch der iRMC S2/S3 konfiguriert werden. Auch die gleichzeitige Konfiguration einer größeren Anzahl von Servern lässt sich Skript-basiert durchführen.

- Unterstützung des LocalView Service Panels

  Bei PRIMERGY Servern, die über ein ServerView Local Service Panel verfügen, können Sie an diesem Modul erkennen, welches Bauteil defekt ist und ob Sie das defekte Bauteil selbst austauschen können.

- Lokale Benutzerverwaltung

Der iRMC S2/S3 verfügt über eine eigene Benutzerverwaltung, mit der bis zu 16 Benutzer mit Kennwörtern angelegt und je nach Gruppenzugehörigkeit mit unterschiedlichen Rechten versehen werden können.

- Globale Benutzerverwaltung mithilfe eines Verzeichnisdienstes

  Die globalen Benutzerkennungen für den iRMC S2/S3 werden zentral abgelegt im Verzeichnis (Directory) eines Verzeichnisdienstes. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten und können somit von allen iRMC / iRMC S2 / iRMC S3 verwendet werden, die mit diesem Server im Netz verbunden sind.

  Für die iRMC S2/S3-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDS

- CAS-basierte Single sign-on (SSO)-Authentifizierung

  Der iRMC S2/S3 unterstützt die Konfiguration des zentralisierten Authentifizierungsdienstes CAS (Centralized Authentication Service). Damit können Sie die iRMC S2/S3 Web-Oberfläche für die CAS-basierte Single sign-on (SSO)-Authentifizierung konfigurieren.

  Wenn sich ein Benutzer das erste Mal bei einer Anwendung (z.B. iRMC S2/S3-Web-Oberfläche) innerhalb der SSO-Domäne des CAS anmeldet, fordert ihn das CAS-spezifische Login-Fenster zur Eingabe seiner Authentisierungsdaten auf. Nach einmaliger erfolgreicher Authentifizierung durch den CAS Service hat der Benutzer dann Zugriff auf die iRMC S2/S3-Web-Oberfläche sowie auf alle weiteren Services innerhalb der SSO-Domäne, ohne dass er jedesmal erneut zur Eingabe seiner Authentisierungsdaten aufgefordert wird.

- DNS / DHCP

  Der iRMC S2/S3 unterstützt die automatische Netz-Konfiguration. Er hat einen Default-Namen, und DHCP-Unterstützung ist standardmäßig eingestellt, sodass der iRMC S2/S3 seine IP-Adresse vom DHCP-Server erhält. Der iRMC S2/S3-Name wird vom Domain Name Service (DNS) registriert. Es werden bis zu fünf DNS-Server unterstützt. Falls DNS/DHCP nicht verfügbar ist, unterstützt der iRMC S2/S3 auch statische IP-Adressen.

- Stromversorgung

  Die Stromversorgung des iRMC S2/S3 erfolgt über die Stand-by-Versorgung des Systems.

- Alarm-Management

  Das Alarm-Management des iRMC S2/S3 bietet folgende Möglichkeiten für die Weiterleitung von Alarmen (Alerting):

  – Platform Event Traps (PET) werden via SNMP versendet.

  – Direkte Benachrichtigung per E-Mail.

  – An die serielle Schnittstelle lässt sich ein Modem anschließen, über das Alarme (Alerts) versendet werden (z.B. per SMS an ein Mobiltelefon).

  Darüber hinaus versorgt der iRMC S2/S3 den ServerView-Agenten mit allen relevanten Informationen.

- Fehlerspeicher (System Eventlog, SEL) auslesen, filtern und speichern.

  Den Inhalt des Fehlerspeichers können Sie filtern, einsehen, speichern und löschen

  – über die iRMC S2/S3-Web-Oberfläche oder

  – über die Telnet/SSH-basierte Schnittstelle (Remote Manager) des iRMC S2/S3.

- Internen Ereignisspeicher (Internal Eventlog) auslesen, filtern und speichern.

  Den Inhalt des internen Ereignisspeichers können Sie filtern, einsehen, speichern und löschen

  – über die iRMC S2/S3-Web-Oberfläche oder

  – über die Telnet/SSH-basierte Schnittstelle (Remote Manager) des iRMC S2/S3.

Erweiterte Funktionalität des iRMC S2/S3

Neben der Standardfunktionalität unterstützt der iRMC S2/S3 zusätzlich die Funktionen „Grafische Konsolen-Umleitung“ (Advanced Video Redirection) und „Remote Storage“.

- Grafische Konsolen-Umleitung (Advanced Video Redirection, AVR)

  Der iRMC S2/S3 unterstützt die grafische Konsolen-Umleitung mit folgenden Vorteilen:

  – Bedienung über einen Standard-Web-Browser. Auf der Management-Station braucht außer dem Java Runtime Environment keine zusätzliche Software installiert zu werden.

  – System-unabhängige Weiterleitung von Grafik- und Text-Konsole (einschließlich Maus und Tastatur).

  – Fernzugriff für die Überwachung des System-Neustarts sowie für BIOS-Administration und Bedienung des Betriebssystems.

  – Die grafische Konsolen-Umleitung unterstützt bis zu zwei gleichzeitige „virtuelle Verbindungen“ für das Arbeiten an einem Server von einem anderen Standort aus. Außerdem minimiert die grafische Konsolen-Umleitung die Netzbelastung durch Hardware- und Video-Komprimierung.

  – „Lokaler Bildschirm Aus“ (Local Monitor Off)-Unterstützung: Während einer AVR-Sitzung kann der lokale Bildschirm des verwalteten PRIMERGY Servers ausgeschaltet werden, um Unbefugte daran zu hindern, Eingaben und Aktionen der AVR -Sitzung am Server-lokalen Bildschirm zu verfolgen.

  – Geringe Bandbreite

    Für den Fall, dass nur eine eingeschränkte Datentransfer-Rate verfügbar ist, können Sie für die Dauer Ihrer aktuellen AVR-Sitzung eine geringere Bandbreite (Bits pro Pixel, BPP) hinsichtlich der Farbtiefe konfigurieren.

- Remote Storage

  Remote Storage stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich physisch am Remote-Arbeitsplatz befindet oder mithilfe eines Remote Storage Servers zentral im Netz bereitgestellt wird.

  Die per Remote Storage verfügbaren „virtuellen“ Laufwerke sind vergleichbar den lokalen Laufwerken einfach zu verwalten und bieten folgende Möglichkeiten:

  – Daten lesen und schreiben.
  – Von RemoteStorage booten.
  – Treiber und kleinere Anwendungen installieren.
  – BIOS Update vom Remote-Arbeitsplatz durchführen (BIOS Update per USB)

  Für die Bereitstellung eines „virtuellen“ Laufwerks am Remote Arbeitsplatz unterstützt Remote Storage folgende Gerätetypen:

  – CD-ROM
  – DVD-ROM
  – Memory Stick
  – Disketten-Abbild
  – CD ISO-Abbild (Image-Datei)
  – DVD ISO-Abbild (Image-Datei)

  Ein Remote Storage Server stellt ein ISO-Abbild (ISO Image) zentral im Netz als „virtuelles“ Laufwerk zur Verfügung.

  Remote Storage ermöglicht alternativ die gleichzeitige Anbindung von bis zu zwei „virtuellen“ Laufwerken am Remote Arbeitsplatz oder die Bereitstellung eines ISO-Abbilds (ISO Image) via Remote Storage Server.

1.3 Kommunikationsschnittstellen des iRMC S2/S3

Der iRMC S2/S3 bietet folgende Kommunikationsschnittstellen:

- **iRMC S2/S3-Web-Oberfläche (Web-Schnittstelle)**

  Die Verbindung zum iRMC S2/S3-Web-Server erhalten Sie über einen Standard-Web-Browser (z.B. Microsoft Internet Explorer, Mozilla Firefox).

  Über die Web-Oberfläche des iRMC S2/S3 haben Sie u.a. Zugriff auf alle Systeminformationen und Informationen der Sensoren wie Lüfterdrehzahlen, Spannungen etc. Sie können die Text-basierte Konsolen-Umleitung konfigurieren oder die grafische Konsolen-Umleitung (Advanced Video Redirection, AVR) starten. Darüber hinaus kann der Administrator die komplette Konfiguration des iRMC S2/S3 über die Web-Schnittstelle abwickeln. Der Zugang zum Web-Server des iRMC S2/S3 kann über HTTPS/SSL abgesichert werden.

  Die Bedienung des iRMC S2/S3 über die Web-Oberfläche ist beschrieben im Kapitel "iRMC S2/S3-Web-Oberfläche" auf Seite 141.

- **Remote Manager: Text-basierte Telnet/SSH-Oberfläche über LAN**

  Den Remote Manager können Sie wahlweise aufrufen

  – über das ServerView Remote Management Frontend,
  – direkt über einen Telnet/SSH-Client.

  Über die alphanumerische Bedienoberfläche des Remote Manager haben Sie u.a. Zugriff auf System-und Sensorinformationen, das Power Management und den Error-Eventlog. Außerdem können Sie die Textkonsolen-Umleitung sowie eine SMASH CLP Shell starten. Wenn Sie den Remote Manager über SSH (Secure Shell) aufrufen, ist die Verbindung zwischen Remote Manager und verwaltetem Server kryptographisch gesichert.

  Die Bedienung des iRMC S2/S3 über den Remote Manager ist beschrieben im Kapitel "iRMC S2/S3 über Telnet/SSH (Remote Manager)" auf Seite 333.

- **Remote Manager (Serial): Text-basierte Schnittstelle über Serial 1**

  Die Oberfläche des Remote Manager (Serial) ist identisch mit der Oberfläche des Remote Manager.

1.4 Kommunikationsprotokolle, die vom iRMC S2/S3 genutzt werden

In Tabelle 1 sind die vom iRMC S2/S3 verwendeten Kommunikationsprotokolle aufgelistet:

Gegenseite der Verbindung	Kommunikationsrichtung	iRMC S2-Seite der Verbindung (Portnummer / Protokoll)
RMCP	→	623/UDP
	←	623/UDP
HTTP port	→	80/TCP
	←	80/TCP
HTTPs port	→	443/TCP
	←	443/TCP
Telnet	→	3172/TCP
	←	3172/TCP
SSH	→	22/TCP
	←	22/TCP
Trap	→	162/UDP
Email	→	25/TCP
	←	25/TCP
Remote Storage	→	5901/TCP
	←	5901/TCP
VNC ports		
Standard port	→	80/TCP
	←	80/TCP
Secure port	→	443/TCP
	←	443/TCP

Tabelle 1: Kommunikationsprotokolle, die vom iRMC S2/S3 genutzt werden

Ab iRMC S2/S3-Firmware Version 5.00 wird der Remote Storage-Port ausschließlich für den Remote Storage Server und die Client-interne Kommunikation genutzt. Die integrierte Remote Storage-Funktionalität (via Java-Applet) verwendet den http-Port.

1.5 IPMI - Technischer Hintergrund

Über die IPMI-Schnittstelle stellt der iRMC S2/S3 die BMC-Funktionalität zur Verfügung.

Intelligent Platform Management

Die Initiative „Intelligent Platform Management“ ist eine Reaktion auf die ansteigende Komplexität moderner Serversysteme. Zahlreiche Hersteller haben sich in dieser Initiative zusammengeschlossen, um eine neue Lösung für die Überwachung dieser Serversysteme zu erarbeiten.

Der Begriff „Intelligent Platform Management“ bringt den Kernaspekt dieses Lösungsansatzes zum Ausdruck: Funktionen zum Überwachen und Wiederherstellen von Systemen werden direkt in die Hard- und Firmware für das Plattform-Management implementiert.

Ziel

Ziel war die Definition einer standardisierten, abstrakten und Mitteilung-basierten Schnittstelle zwischen dem zentralen System-Controller (Baseboard Management Controller - BMC) und intelligenter Hardware zum Plattform-Management.

Dabei fassten die Standardisierungsgremien die zentralen Charakteristika verschiedener Baugruppen zum Plattform-Management in standardisierende Beschreibungen.

Definition

Die IPMI-Spezifikation definiert:

> „IPMI is a hardware level interface specification that is ’management software neutral’ providing monitoring and control functions that can be exposed through standard management software interfaces such as DMI, WMI, CIM, SNMP, etc. As a hardware level interface, it sits at the bottom of a typical management software stack“ [siehe Abschnitt "IPMI und andere Management-Standards" auf Seite 23].

Vorteil

Die IPMI-Spezifikationen sichern die Unabhängigkeit der Funktionen zu Inventory, Logging, Recovery und Überwachung eines Systems vom Prozessor, BIOS oder Betriebssystem des Systems.

Damit kann ein System auch in das Plattform-Management einbezogen werden, wenn es heruntergefahren und ausgeschaltet ist.

IPMI und andere Management-Standards

Am besten kann IPMI genutzt werden in Verbindung mit einer Software zum System-Management, die unter dem Betriebssystem läuft. Mit der Integration der IPMI-Funktionalität in die Managementfunktionalität, die eine Management-Applikation und das Betriebssystem bieten, entsteht eine mächtige Umgebung zum Plattform-Management.

Eine Übersicht zum Verhältnis von IPMI zum Management-Software-Stack zeigt Bild 2:

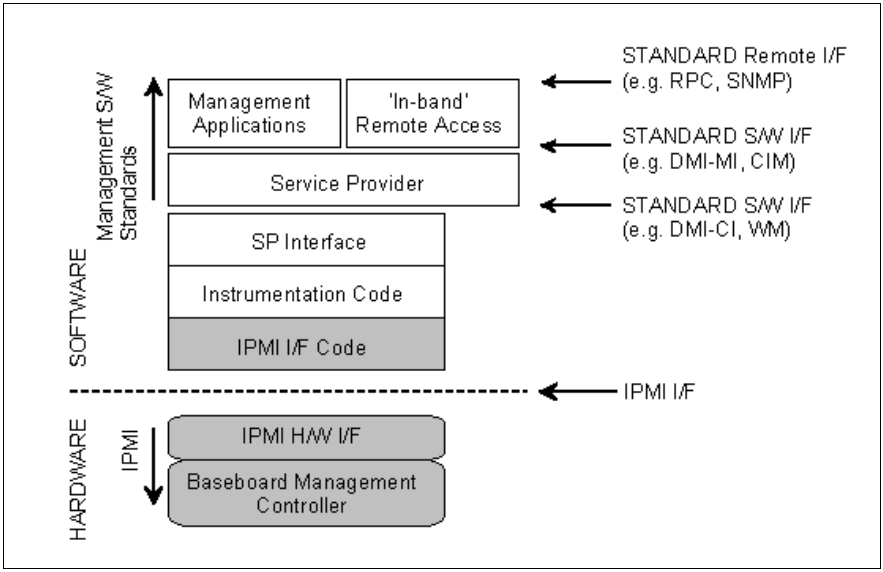


Bild 2: IPMI im Management-Software-Stack (Quelle: IPMI Specification, siehe Abschnitt "Referenzen" auf Seite 30)

IPMI, IPMB und ICMB

Im Rahmen der IPMI-Initiative entstanden drei zentrale Standards:

– *IPMI. Intelligent Platform Management Interface Specification*
beschreibt die übergeordnete Architektur, die gängigen Kommandos, Ereignisformate, Datenpakete und Eigenschaften, die in IPMI-basierten Systemen zum Einsatz kommen.

– *IPMB. Intelligent Platform Management Bus*
ist ein I^2C-basierter (write only) Bus, der eine standardisierte Verbindung herstellt zwischen verschiedenen Baugruppen in einem Gehäuse.
Der IPMB kann auch als standardisierte Schnittstelle für Remote-Management-Baugruppen eingesetzt werden.

– *ICMB. Intelligent Chassis Management Bus*
(Derzeit im ServerView Remote Management-Umfeld nicht implementiert.) bietet eine standardisierte Schnittstelle für den Austausch von Information zum Plattform-Management und zur Kontrolle zwischen Systemen. Der ICMB ist so entworfen, dass er mit einem Gerät implementiert werden kann, das an den IPMB angeschlossen wird.

IPMI Implementierung

Kernelement einer IPMI-Implementierung ist der Baseboard Management Controller (BMC).
Der BMC erfüllt folgende Aufgaben:

– Der BMC organisiert die Schnittstelle zwischen der Software für das System-Management und der Hardware für das Plattform-Management.

– Er bietet autonome Funktionen für die Überwachung, das Event-Logging und die Recovery-Kontrolle.

– Der BMC dient als Gateway zwischen der Software zum System-Management und IPMB.

IPMI ermöglicht das Erweitern von Plattform-Management: Über den IPMB können zusätzliche Management-Controller angebunden werden. Der IPMB ist ein I^2C-basierter serieller Bus, der zwischen den Hauptmodulen des Systems verläuft. Er wird für die Kommunikation mit und zwischen den Management-Controllern genutzt.

Mit der Unterstützung mehrerer Management-Controller bietet IPMI eine skalierbare Architektur: Ein komplexes Server-System kann mehrere Controller für die Überwachung verschiedener Subsysteme nutzen, z.B. der Stromversorgungen, der hot-swap RAID-Laufwerkseinschübe, usw.

Darüberhinaus bietet IPMI 'low-level' I^2C-Kommandos, mit denen über einen am IPMB angeschlossenen Management-Controller zugegriffen werden kann auf 'unintelligente' I^2C-Baugruppen, die keine IPMI-Kommandos verarbeiten.

Einen Überblick über die grundlegenden Elemente einer IPMI-Implementierung bietet Ihnen Bild 3 auf Seite 26.

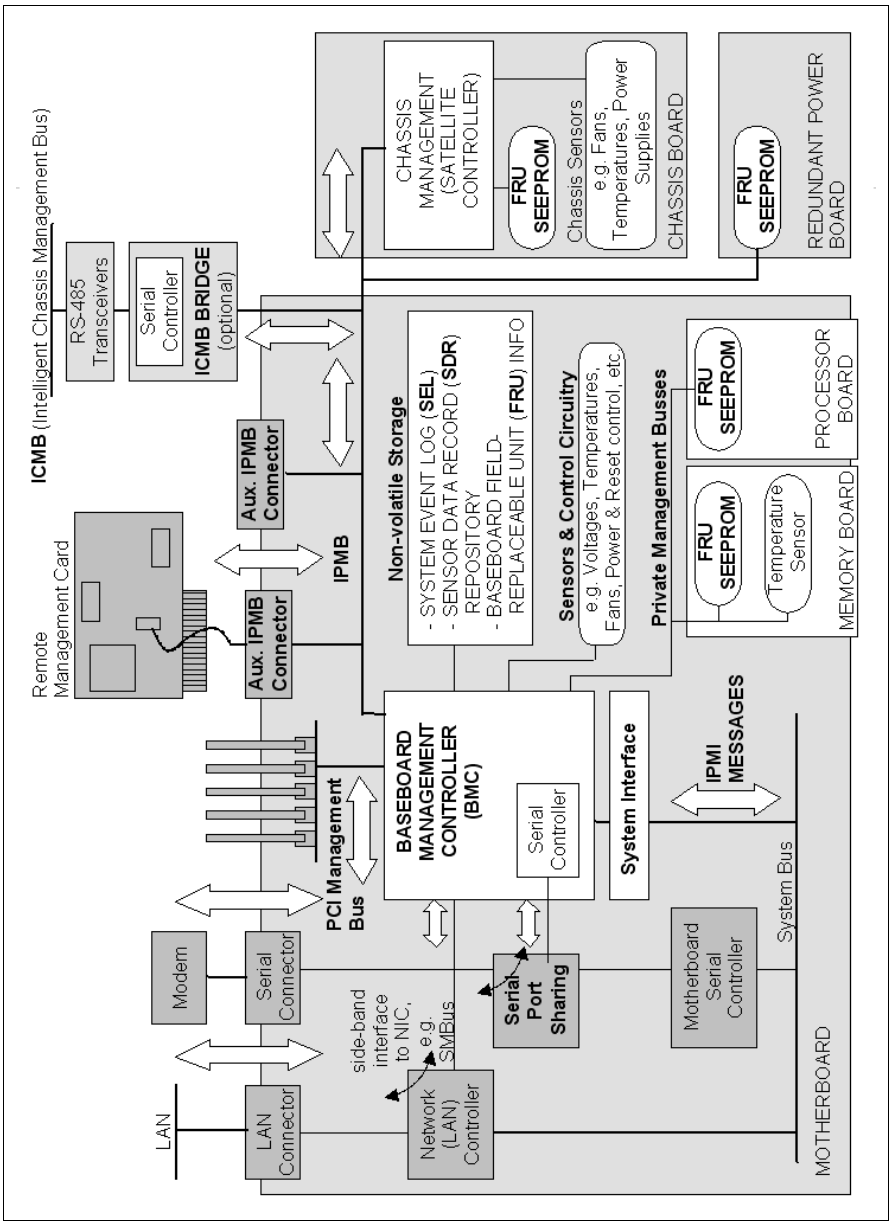


Bild 3: IPMI Blockdiagramm (Quelle: IPMI Specification, siehe Abschnitt "Referenzen" auf Seite 30)

IPMI und „in-band“ und „out-of-band“ Management

Im System-Management-Umfeld wird unterschieden zwischen „in-band“-Management und „out-of-band“-Management:

– „in-band“-Management findet statt, wenn das Betriebssystem am verwalteten Server läuft.

– „out-of-band“-Management findet statt, wenn das Betriebssystem am verwalteten Server nicht läuft, z.B. weil Hardware defekt ist.

Mit den verschiedenen Schnittstellen, die ein IPMI-fähiges System zur Verfügung stellt, lassen sich IPMI-fähige Systeme sowohl „in-band“ als auch „out-of-band“ verwalten.

IPMI-over-LAN

"IPMI-over-LAN" ist die gängige Bezeichung für die Spezifikation der LAN-Schnittstelle im IPMI-Standard. Diese Spezifikation legt fest, wie IPMI-Mitteilungen an bzw. von dem BMC eines verwalteten Systems gesendet werden können - verkapselt in RMCP (Remote Management Control Protocol)-Datenpakete. Diese RMCP-Datenpakete werden übertragen über eine Ethernet-LAN-Verbindung über das UDP (User Datagram Protocol) unter IPv4 (Internet Protocol Version 4).

Das RMCP-Protokoll wurde spezifiziert, um das Management von Systemzuständen zu unterstützen, in denen das Betriebssystem nicht läuft. Das RMCP ist ein einfaches Frage-Antwort-Protokoll.

Die Schnittstelle für eine solche Verbindung wird bereitgestellt über einen onboard LAN-Controller, der dem BMC zugeordnet ist.

Die Schnittstelle kann nur über einen onboard LAN-Controller zur Verfügung gestellt werden, nicht über eine gesteckte LAN-Karte.

Von den zwei Ports, die RCMP unter UDP nutzt, kommuniziert der BMC mit dem LAN-Controller über den Port 623 (Primary RMCP Port).

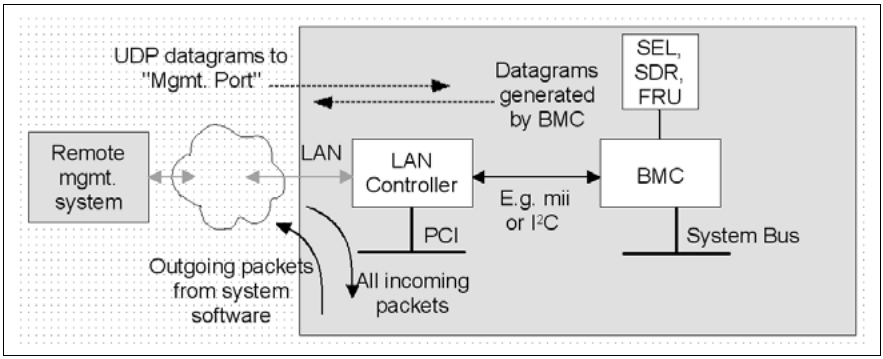


Bild 4: BMC und LAN-Controller

Serial Over LAN-Schnittstelle (SOL)

"Serial Over LAN" ist eine Schnittstelle im IPMI V2.0-Standard, die die Übertragung serieller Daten über eine LAN-Verbindung regelt. Im Einzelnen spezifiziert SOL dabei die Paketformate und Protokolle für den LAN-Transfer serieller Datenströme zwischen dem Serial Controller am verwalteten Rechner und einem Remote-Arbeitsplatz. SOL basiert auf der IPMI-over-LAN-Spezifikation.

Zur Einrichtung einer SOL-Verbindung initiiert eine Remote-Management-Anwendung zunächst eine IPMI-over-LAN-Session mit dem BMC. Danach können die SOL-Dienste vom Remote-Arbeitplatz aus aktiviert werden. Der Datenverkehr zwischen dem Serial Controller und dem Remote-Arbeitsplatz wird über dieselbe IPMI-Session abwickelt, über die auch die IPMI-Kommandos abgewickelt werden.

Sobald eine SOL-Verbindung eingerichtet ist, verläuft der Datentransfer zwischen Serial Controller und Remote Arbeitsplatz nach folgendem Schema:

– Transfer vom Serial Controller an den Remote-Arbeitsplatz:
  Der vom Serial Controller ausgehende Datenstrom wird vom BMC partitioniert, in Pakete "verpackt" und über LAN an den Remote-Arbeitsplatz gesendet.

– Transfer vom Remote-Arbeitsplatz an den Serial Controller:
  Die Zeichen, die in den vom Remote-Arbeitsplatz gesendeten Paketen enthalten sind, werden vom BMC entpackt und als Zeichenstrom an den Serial Controller weitergeleitet.

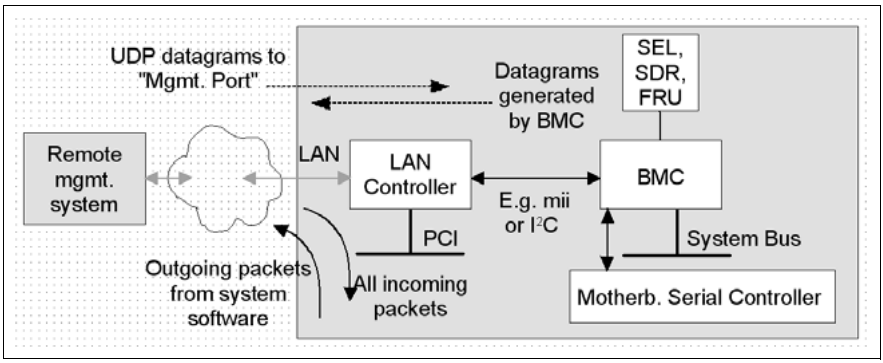


Bild 5: BMC und SOL

Die SOL-Zeichendaten werden als SOL-Mitteilungen zwischen dem BMC des verwalteten Systems und dem Remote-Arbeitsplatz ausgetauscht. Verkapselt in RMCP+-Datenpakete werden SOL-Mitteilungen in UDP Datagrammen übertragen über eine Ethernet-LAN-Verbindung unter IPv4 (Internet Protocol Version 4). Das RMCP+-Protokoll basiert auf dem RMCP-Protokoll, enthält jedoch Erweiterungen u.a. für Verschlüsselung und Authentifizierung.

Serial Over LAN ermöglicht "headless" Management durch Konsolumleitung sowohl des BIOS als auch des Betriebssystems des verwalteten Servers. Kostenintensive Konzentratorlösungen werden nicht benötigt.

Kanal-Konzept unter IPMI

'Kanäle' stellen die Mechanismen zur Verfügung, mit denen IPMI-Meldungen über verschiedene Verbindungsträger zum BMC geleitet werden. Es können bis zu neun Kanäle unterstützt werden. Die Systemschnittstelle und der Primary IPMB sind festgelegt. Die anderen sieben Kanäle stehen der Implementierung offen.

Kanäle können 'session-based' oder 'session-less' sein. Das Konzept 'Sitzung' hat zwei Zielrichtungen: Entweder ein Konzept zur Benutzer-Authentifizierung (siehe Abschnitt "Benutzerkennungen" auf Seite 30) oder ein Konzept, um mehrere IPMI-Meldungs-Ströme über einen einzelnen Kanal zu leiten.

Beispiele für ’session-based’ Kanäle sind LAN-Kanäle oder serielle oder Modem-Kanäle. Beispiele für ’session-less’ Kanäle sind die Systemschnittstelle und der IPMB.

Benutzerkennungen

Für ’session-based’ Kanäle (siehe Abschnitt "Kanal-Konzept unter IPMI" auf Seite 29) ist eine Nutzeranmeldung notwendig. Die ’session-less’ Kanäle haben dagegen keine Benutzer-Authentifizierung.

Unter IPMI ist die Konfiguration der Benutzer Kanal-spezifisch. So kann ein Benutzer verschiedene Rechte haben, je nachdem ob er auf den BMC über den LAN-Kanal oder über den seriellen Kanal zugreift.

Referenzen

Informationen zu den IPMI-Standards finden Sie im Internet:

http://developer.intel.com/design/servers/ipmi/index.htm

1.6 DCMI (Data Center Management Interface)

Der iRMC S2/S3 unterstützt das DCMI (Data Center Management Interface)-Protokoll, das konform zum IPMI V2.0-Standard ist. Ziel von DCMI ist es, Administrierbarkeit und Energieeffizienz von Servern in großen Datencentern zu optimieren.

Zur Unterstützung des Hardware-Managements von Servern in Datencentern bietet DCMI u.a. folgende Schlüsselfunktionen:

– Inventory-Funktionen (Server-Identifikation)
– Energieverwaltung und -überwachung
– Überwachung und Steuerung des Energieverbrauchs
– Event-Logging
– Temperaturüberwachung

Detaillierte Informationen finden Sie auf der DCMI-Hompage:

http://www.intel.com/technology/product/DCMI

1.7 Änderungen gegenüber den vorherigen Ausgaben

iRMC S2/S3 - integrated Remote Management Controller (Ausgabe Juli 2012)

Dieses Handbuch bezieht sich auf die iRMC S2/S3-**Firmware version 6.5x** und löst das folgende Online-Handbuch ab: “iRMC S2/S3 - integrated Remote Management Controller”, Ausgabe Mai 2012, das nur in englischer und japanischer Sprache verfügbar ist.

Das Handbuch enthält folgende Erweiterungen:

- In Kapitel "7 iRMC S2/S3 Web -Oberfläche" wird Funktion "0 Watt Technologie" beschrieben.
- Das frühere Kapitel "12 IPMI OEM-Kommandos" wurde erweitert, wird jetzt als Anhang geführt ("12 Anhang") und enthält die folgenden Abschnitte:
  - "12.1 Vom iRMC S2/S3 unterstützte IPMI OEM-Kommandos" (ehemaliges Kapitel "12 IPMI OEM-Kommandos")
  - "12.2 Konfiguration des iRMC S2/S3 via SCCI und Script-basierte Konfiguration" (neuer Abschnitt).

iRMC S2/S3 - integrated Remote Management Controller (Ausgabe Mai 2012, nur in englischer und japanischer Sprache verfügbar)

Dieses Handbuch bezieht sich auf die iRMC S2/S3-**Firmware version 6.5x** und löst das folgende Online-Handbuch ab: “iRMC S2/S3 - integrated Remote Management Controller”, Ausgabe November 2011.

Neue Funktionen des iRMC S2/S3 (beschrieben in Kapitel "7 iRMC S2/S3 Web-Oberfläche"):

- Agentenless HDD Monitoring (nur iRMC S3)

  Wenn der verwaltete Server die Funktion "Agentless HDD Monitoring" unterstützt, wird der Status HDD<n> jedes einzelnen Festplattenlaufwerks (Hard Disk Drive, HDD) direkt ausgelesen und zum direkt zu iRMC S3 übertragen und kann auch dann angezeigt werden, wenn keine ServerView-Agenten ausgeführt werden.

- BIOS Parameter sichern und wiederherstellen

  Sofern das BIOS des verwalteten Servers die entsprechenden funktionalen Anforderungen unterstützt, ermöglicht der iRMC S2/S3 die Durchführung der folgenden Aktionen:

  – Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format abspeichern und diese Parameter im ServerView® WinSCU XML-Format aus einer Datei wiederherstellen.

  – BIOS aktualisieren via "Hochladen aus Datei" oder via TFTP.

- Bei einigen Server-Typen können Sie unter *Optionen der Energieverbrauchsbegrenzung* den Modus *Begrenzung des Geräuschpegels* auswählen (nur iRMC S3).

iRMC S2/S3 - integrated Remote Management controller (Ausgabe November 2011)

Dieses Handbuch bezieht sich auf die iRMC S2/S3-**Firmware version 5.5x** und löst das folgende Online-Handbuch ab: “iRMC S2/S3 - integrated Remote Management Controller”, Ausgabe Mai 2011.

Die folgenden Themen sind nicht mehr Bestandteil dieses Handbuchs:

– Ehemaliger Abschnitt „4.4 Globale Benutzerverwaltung für den iRMCS2/S3“. Ab ServerView Operations Manager V5.50 ist die entsprechende Beschreibung im Handbuch „Benutzerverwaltung in ServerView“ enthalten.

– Beschreibung der Dialoge des Server Configuration Managers (ehemals Abschnitt 9.2 und folgende). Stattdessen wird der Leser auf die Online-Hilfe des Server Configuration Managers verwiesen.

iRMC S2/S3 - integrated Remote Management controller (Ausgabe Mai 2011)

Dieses Handbuch bezieht sich auf die iRMC S2/S3-**Firmware version 5.5x** und löst das folgende Online-Handbuch ab: “iRMC S2 - integrated Remote Management Controller”, Ausgabe Juli 2010.

Das Handbuch gilt gleichermaßen für iRMC S2 und iRMC S3. Funktionelle Unterschiede zwischen iRMC S2 und iRMC S3 sind im Handbuch gesondert ausgewiesen.

Zu den funktionellen Änderungen gegenüber der Ausgabe Juli 2010 siehe nachfolgendes Änderungsprotokoll zu „iRMC S2 - integrated Remote Management Controller (Ausgabe April 2011, nur in englischer Sprache verfügbar)“.

iRMC S2 - integrated Remote Management Controller (Ausgabe April 2011, nur in englischer Sprache verfügbar)

Die April 2011-Ausgabe des iRMC S2-Handbuchs bezieht sich auf die iRMC S2-**Firmware version 5.5x** und löst das folgende Online-Handbuch ab: “iRMC S2 - integrated Remote Management Controller”, Ausgabe Juli 2010.

- Neue iRMC S2-Funktionen:
  - Zusätzlich zum System Event-Log (IPMI SEL) bietet der iRMC S2 einen internen Event-Log.
  - Der iRMC S2 unterstützt IPv4- und IPv6-Adressen.
  - Der iRMC S2 unterstützt den Verzeichnisdienst Open DS.
  - Die iRMC S2 -Konfiguration (iRMC S2 Firmware-Einstellungen) kann via iRMC S2/S3-Web-Oberfläche wiederhergestellt werden.
  - Email-Benachrichtigung wird jetzt auch für globale iRMC S2-Benutzerkennungen unterstützt.
- Kapitel "5 Grafische Konsolen-Umleitung (AVR)":

  Neben einigen kleineren Änderungen wurde das Menü des AVR-Fensters um den Menü-Punkt *Ein-/Ausschalten* erweitert, über den Sie den Server direkt aus dem AVR-Fenster einschalten / ausschalten / neu starten können.
- Kapitel "7 iRMC S2-Web Oberfläche":
  - Seite *Netzteil*: Die Funktion *Konfiguration der Stronmversorgung Redundanz* wird für einige Server-Typen unterstützt.
  - Seite *Fehlerliste*:

    GUI-Sprache "Deutsch":
    Fehlerbeschreibung und Lösungsvorschläge werden in deutscher Sprache angeboten.

    GUI-Sprache "Japanisch":
    Lösungsvorschläge werden in japanischer Sprache angeboten
  - Die Seite *DNS Konfiguration* page umfasst n zusätzlich die Funktionalität der ehemaligen Seite *DHCP Konfiguration* page, die nicht mehr verfügbar ist.
  - Neue / modifizierte Seiten entsprechend der oben erwähnten neuen iRMC S2-Funktionen.

1.8 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt Ihnen über die Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Handbücher
- Service Desk
- Produktinformationen
- Schulungen
- Sicherheitsinformationen
- Software Downloads

Die Downloads umfassen u.a.:

- aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.
- Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView-Agenten und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
- die aktuellen Versionen aller Dokumentationen zur ServerView Suite

Die Downloads können kostenlos vom Fujitsu Technology Solutions Web-Server heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Ersatzteilkatalog
- Handbücher
- Service Desk
- Produktinformationen

Zugriff auf die ServerView Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. über den ServerView Operations Manager

   ► Wählen Sie auf der Startseite bzw. in der Menüzeile *Help – Links* aus.

   Anschließend wird die Startseite der Link-Sammlung angezeigt.

2. über die ServerView Suite DVD 2 bzw. über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions

   Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

   http://manuals.ts.fujitsu.com

   ► Wählen Sie links in der Auswahlliste *Industry standard servers* aus.

   ► Klicken Sie auf den Menüpunkt *PRIMERGY ServerView Links*.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

3. über die ServerView Suite DVD 1

   ► Markieren Sie im Startfenster der ServerView Suite DVD 1 die Option *ServerView Software Produktauswahl*.

   ► Klicken Sie auf *Starten*. Sie gelangen auf die Seite der Software Produkte der ServerView Suite.

   ► Wählen Sie in der Menüleiste *Links*.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

1.9 Dokumentation zur ServerView Suite

Die Dokumentation zur ServerView Suite finden Sie auf der ServerView Suite DVD 2, die mit jedem Server ausgeliefert wird.

Die Dokumentation ist auch über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation zur ServerView Suite finden Sie unter *http://manuals.ts.fujitsu.com* und dem Link *Industry standard servers*.

1.10 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

Warnung	Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben.
►	Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt.
Kursive Schrift	Im Fließtext werden Kommandos, Menüpunkte, die Namen von Schaltflächen, Optionen, Dateinamen und Pfadnamen *kursiv* dargestellt.
<Schrift>	Kennzeichnet Variablen, die durch aktuelle Werte ersetzt werden müssen.
`dicktengleich`	Ausgaben des Systems werden `dicktengleich` dargestellt.
`dicktengleich halbfett`	Über die Tastatur einzugebende Anweisungen werden dicktengleich halbfett dargestellt.
[eckige Klammern]	Kennzeichnen optionale Eingaben.
{geschweifte Klammern}	Kennzeichnen eine Liste Alternativen, die durch „|“ voneinander getrennt sind.
Tastensymbole	Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z. B. SHIFT - A für A. Müssen zwei Tasten gleichzeitig gedrückt werden, so wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet.

Tabelle 2: Darstellungsmittel

Wird auf Textstellen in diesem Handbuch verwiesen, so wird die Überschrift des Kapitels bzw. Abschnitts genannt, wobei sich die Seitenangabe auf den Beginn des Abschnitts bezieht.

2 Zum ersten Mal am iRMC S2/S3 anmelden

Der iRMC S2/S3 bietet Voreinstellungen, mit denen Sie sich ohne weitere Konfigurationsschritte das erste Mal am iRMC S2/S3 anmelden können.

2.1 Voraussetzungen

Am Remote-Arbeitsplatz:

– Windows: Internet Explorer ab Version 7.x;
  Linux: Mozilla Firefox 3.x.

– Für die Konsolumleitung:
  Sun Java Virtual Machine 1.5.0_06 oder in einer höheren Version.

In Ihrem Netz:

– Im Ihrem Netz muss sich ein DHCP-Server befinden.

– Wenn Sie sich an der iRMC S2/S3-Web-Oberfläche an Stelle einer IP-Adresse über einen symbolischen Namen anmelden möchten, muss der DHCP-Server in Ihrem Netz für dynamischen DNS konfiguriert sein.

– DNS muss konfiguriert sein. Andernfalls müssen Sie die IP-Adresse erfragen.

2.2 iRMC S2/S3-Voreinstellungen

Die Firmware des iRMC S2/S3 stellt eine Standard-Administratorkennung und einen Standard-DHCP-Namen für den iRMC S2/S3 zur Verfügung.

Standard-Administratorkennung:

Administratorkennung: admin

Passwort: admin

Für Administratorkennung und Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

Es wird dringend empfohlen, nach der Anmeldung aus Sicherheitsgründen eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Passwort der Kennung zu ändern (siehe Abschnitt "Benutzerverwaltung" auf Seite 272).

Standard-DHCP-Name für den iRMC S2/S3

Der Standard-DHCP-Name für den iRMC S2/S3 folgt dem Muster: *IRMC<Seriennummer>*

Die Seriennummer entspricht den letzten 3 Bytes der MAC-Adresse des iRMC S2/S3. Die MAC-Adresse des iRMC S2/S3 können Sie dem Aufkleber auf Ihrem PRIMERGY Server entnehmen.

Nach dem Anmelden finden Sie die MAC-Adresse des iRMC S2/S3 als unveränderlichen Eintrag oberhalb der Eingabefelder in der Seite *Netzwerk Schnittstelle* (siehe Seite 245).

2.3 An der iRMC S2/S3-Web-Oberfläche anmelden

► Öffnen Sie am Remote-Arbeitsplatz einen Web-Browser und geben Sie den DNS-Namen oder die IP-Adresse des iRMC S2/S3 ein.

Den DNS-Namen des iRMC S2/S3 können Sie dem Aufkleber auf Ihrem PRIMERGY Server entnehmen.

Es wird dann der folgende Anmeldebildschirm angezeigt:

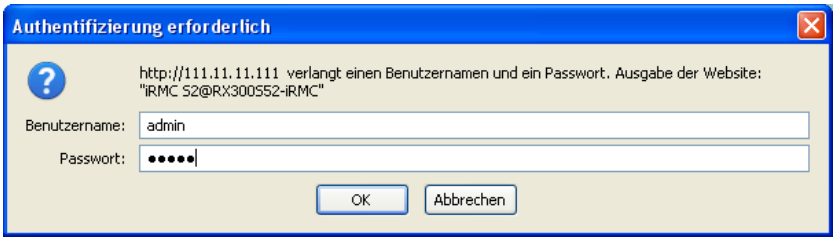


Bild 6: Anmeldebildschirm der iRMC S2/S3-Web-Oberfläche

Falls der Anmeldebildschirm nicht angezeigt wird, überprüfen Sie die LAN-Verbindung (siehe Abschnitt "LAN-Schnittstelle testen" auf Seite 49).

► Geben Sie die Daten der Standard-Administratorkennung ein:

Benutzername: admin

Passwort: admin

► Um zu bestätigen, klicken Sie auf die Schaltfläche *OK*.

Die iRMC S2/S3-Web-Oberfläche öffnet sich, die Seite *System Information* (siehe Seite 152) wird angezeigt.

3 iRMC S2/S3 konfigurieren

Für die Konfiguration des iRMC S2/S3 stehen folgende Tools zur Verfügung:

– BIOS / TrustedCore / UEFI Setup Utility (siehe Seite 46)

– iRMC S2/S3-Web-Oberfläche (siehe Seite 141)

– Server Configuration Manager (siehe Seite 359)

Dieses Kapitel informiert über folgende Themen:

– LAN-Schnittstelle des iRMC S2/S3 über das BIOS / Trusted Core / UEFI Setup Utility konfigurieren (siehe Seite 46).

– Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren (siehe Seite 50).

– Serielle Schnittstelle des iRMC S2/S3 über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren (siehe Seite 59).

– iRMC S2/S3 über die Web-Oberfläche konfigurieren (Überblick, siehe Seite 66).

3.1 LAN-Schnittstelle des iRMC S2/S3 konfigurieren

Dieser Abschnitt beschreibt:

– Voraussetzungen für die Konfiguration der LAN-Schnittstelle

– LAN-Schnittstelle im BIOS Setup konfigurieren

– LAN-Schnittstelle testen

Für den Switch-Port zum Anschluss des iRMC S2/S3 muss „Spanning Tree“ deaktiviert sein (z.B. Port Fast=enabled; Fast Forwarding= enabled).

3.1.1 Voraussetzungen

Beachten Sie folgende Voraussetzungen für das Konfigurieren der IP-Adresse:

– Die LAN-Verbindung muss am richtigen Port gesteckt sein (siehe Abschnitt "An der richtigen LAN-Schnittstelle gesteckt?" auf Seite 44).

– Zusammenspiel der IP-Adressen des iRMC S2/S3 und des Systems (siehe Abschnitt "Zusammenspiel der IP-Adressen des iRMC S2/S3 und des Systems" auf Seite 45).

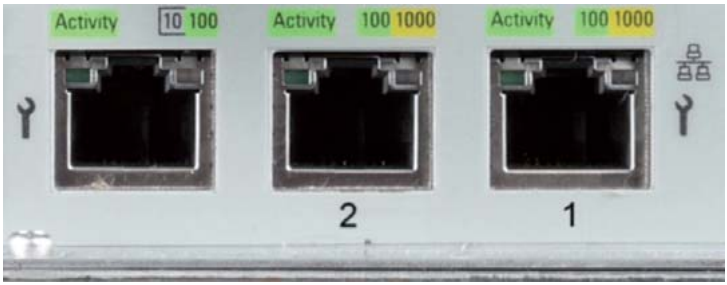
3.1.1.1 An der richtigen LAN-Schnittstelle gesteckt?

Die Schnittstelle für eine LAN-Verbindung wird bereitgestellt über einen onboard LAN-Controller, der dem iRMC S2/S3 zugeordnet ist (vergleiche Bild 4 auf Seite 28).

Die Systembaugruppe eines PRIMERGY Servers stellt je nach Typ des Servers zwei oder drei LAN-Schnittstellen zur Verfügung. Dem iRMC S2/S3 zugeordnet sind die Ports, die mit dem Symbol eines Schraubenschlüssels gekennzeichnet sind (in Bild 7 sind dies Port 1 und der linke obere Port).

Prüfen Sie, ob die LAN-Verbindung am richtigen Port gesteckt ist!

Je nach Typ des PRIMERGY Servers können unterschiedliche Ports mit dem Schraubenschlüssel-Symbol gekennzeichnet sein.



Dediziertes Service / Management LAN
(Port exklusiv reserviert für den iRMC S2/S3; mit dem iRMC S3 ist eine LAN Geschwindigkeit bis zu 1000 MBit/s verfügbar (abhängig von der Server Hardware).

(1) Shared LAN (iRMC S2/S3 und System)

(2) LAN (Port ist exklusiv für das System reserviert.)

Bild 7: Ports für den iRMC S2/S3 (mit Schraubenschlüssel-Symbol gekennzeichnet)

3.1.1.2 Zusammenspiel der IP-Adressen des iRMC S2/S3 und des Systems

Der LAN-Controller des PRIMERGY Servers verlangt eine eigene IP-Adresse für den iRMC S2/S3, um eine sichere Zustellung von Datenpaketen an den iRMC S2/S3 (und nicht an das Betriebssystem) zu gewährleisten.

Die IP-Adresse des iRMC S2/S3 muss sich von der des Systems (Betriebssystems) unterscheiden.

3.1.1.3 Zugriff aus einem anderen Sub-Netz

Wenn der Remote-Arbeitsplatz aus einem anderen Sub-Netz auf den iRMC S2/S3 des verwalteten Servers zugreift und kein DHCP verwendet wird, müssen Sie das Gateway konfigurieren.

3.1.2 LAN-Schnittstelle konfigurieren: Konfigurationstools

Je nach Server-Typ können Sie die LAN-Schnittstelle des iRMC S2/S3 wahlweise wie folgt konfigurieren:

– über das BIOS Setup Utility oder das TrustedCore® Setup Utility (siehe Seite 46),

– über die iRMC S2/S3-Web-Oberfläche (siehe Abschnitt "Netzwerk Einstellungen - LAN-Parameter des iRMC S2/S3 konfigurieren" auf Seite 244),

– über den Server Configuration Manager (siehe Kapitel "iRMC S2/S3 via Server Configuration Manager konfigurieren" auf Seite 359)

3.1.3 LAN-Schnittstelle des iRMC S2/S3 mit dem BIOS / TrustedCore / UEFI Setup Utility konfigurieren

Die LAN-Schnittstelle Ihres iRMC S2/S3 können Sie dem BIOS / TrustedCore / UEFI Setup Utility konfigurieren:

– Die LAN-Schnittstelle des iRMC S2 konfigurieren Sie mit dem BIOS / TrustedCore Setup Utility.

– Die LAN-Schnittstelle des iRMC S3 konfigurieren Sie mit dem UEFI (**U**nified **E**xtensible **F**irmware **I**nterface) Setup Utility

3.1.3.1 LAN-Schnittstelle des iRMC S2 über das BIOS / TrustedCore Setup Utility konfigurieren

IPv6-Adressen werden im BIOS / TrustedCore Setup Utility nicht unterstützt.

▶ Rufen Sie das BIOS bzw. TrustedCore Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.

▶ Rufen Sie das Menü für die Konfiguration der LAN-Parameter auf:

– BIOS: *Advanced – IPMI – LAN Settings*

– TrustedCore: *Server – IPMI – LAN Settings*

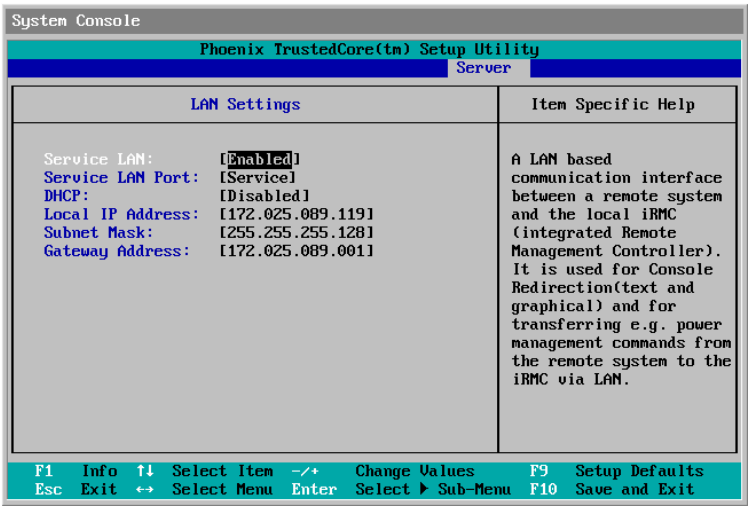

System Console
Phoenix TrustedCore(tm) Setup Utility
Server
LAN Settings
Item Specific Help
Service LAN: [Enabled]
Service LAN Port: [Service]
DHCP: [Disabled]
Local IP Address: [172.025.089.119]
Subnet Mask: [255.255.255.128]
Gateway Address: [172.025.089.001]
A LAN based communication interface between a remote system and the local iRMC (integrated Remote Management Controller). It is used for Console Redirection(text and graphical) and for transferring e.g. power management commands from the remote system to the iRMC via LAN.
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

Bild 8: Menü LAN Settings (hier: Darstellung im TrustedCore Setup Utility)

► Konfigurieren Sie folgende Einstellungen:

Service LAN
Setzen Sie die Einstellung auf *Enabled*.

Service LAN Port
Es wird die Einstellung *Service* empfohlen.

> **i** Für PRIMERGY Server des Typs TX150 S6 ist die Einstellung *Service* zwingend erforderlich.

DHCP
Wenn Sie DHCP aktivieren, erfragt der iRMC S2/S3 eigenständig seine LAN-Einstellungen bei einem DHCP-Server im Netzwerk. In diesem Fall werden die Werte *Local IP Address*, *Subnet Mask* usw. automatisch gesetzt.

> **i** Aktivieren Sie DHCP nicht, wenn kein DHCP-Server verfügbar ist. Wenn Sie DHCP aktivieren und es ist kein DHCP-Server verfügbar, läuft der iRMC S2/S3 in eine Suchschleife (d.h. er sucht endlos nach einem DHCP-Server).
>
> Die Nutzung der Dienste DHCP und DNS können Sie nach der Erstinstallation z.B. über die iRMC S2/S3-Web-Oberfläche konfigurieren (siehe Abschnitt "DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren" auf Seite 256.
> Standardmäßig wird bei der Erstinstallation für den iRMC S2/S3 folgende Bezeichnung an den DHCP-Server weitergegeben: *iRMC<letzte 3Bytes der MAC-Adresse>*.

Local IP Address
Geben Sie die recherchierte IP-Adresse für den iRMC S2/S3 des verwalteten Systems an.

Subnet Mask
Geben Sie die Subnetz-Maske des Netzwerks an.

Gateway Address
Geben Sie hier die IP-Adresse des Gateways an.

► Sichern Sie die Einstellungen.

► Wenn Sie die Konsolen-Umleitung über den iRMC S2/S3 nutzen möchten, fahren Sie fort mit Abschnitt "Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren" auf Seite 50.

Wenn Sie die Text-Konsolen-Umleitung über den iRMC S2/S3 nicht nutzen möchten, beenden Sie das BIOS / TrustedCore Setup und fahren Sie fort mit dem nachfolgenden Abschnitt "LAN-Schnittstelle testen".

3.1.3.2 LAN-Schnittstelle des iRMC S3 über das UEFI Setup Utility konfigurieren

► Rufen Sie das UEFI Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.

► Rufen Sie das Menü *iRMC LAN parameter configuration* auf:

Server Mgmt – iRMC LAN Parameters Configuration

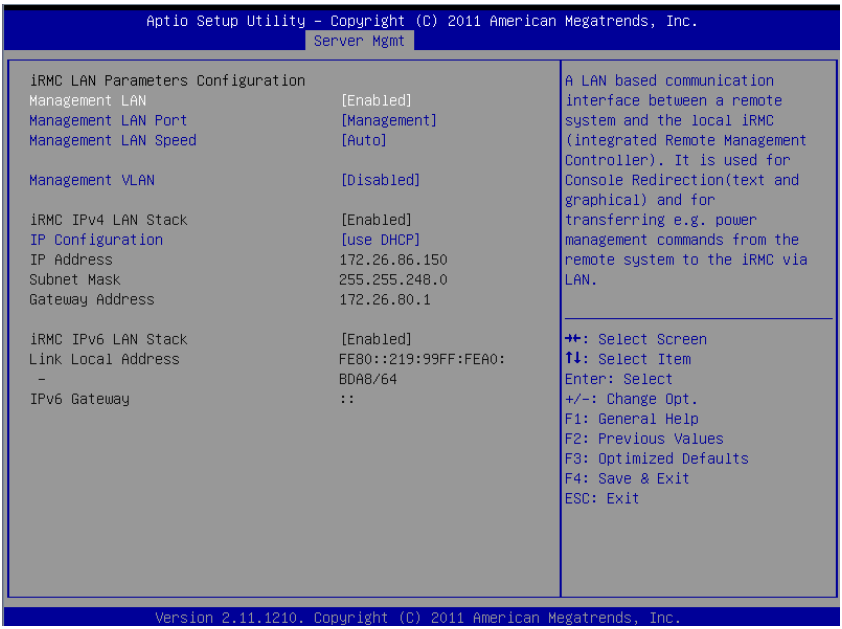

Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc.
Server Mgmt
iRMC LAN Parameters Configuration
Management LAN [Enabled]
Management LAN Port [Management]
Management LAN Speed [Auto]
Management VLAN [Disabled]
iRMC IPv4 LAN Stack [Enabled]
IP Configuration [use DHCP]
IP Address 172.26.86.150
Subnet Mask 255.255.248.0
Gateway Address 172.26.80.1
iRMC IPv6 LAN Stack [Enabled]
Link Local Address FE80::219:99FF:FEA0:
- BDA8/64
IPv6 Gateway ::
A LAN based communication interface between a remote system and the local iRMC (integrated Remote Management Controller). It is used for Console Redirection(text and graphical) and for transferring e.g. power management commands from the remote system to the iRMC via LAN.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.

Bild 9: Menü iRMC LAN Parameters Configuration

► Konfigurieren Sie folgende Einstellungen:

Management LAN
Setzen Sie die Einstellung auf *Enabled*.

Management LAN Port
Es wird die Einstellung *Management* empfohlen.

Für die Konfiguration der restlichen Einstellungen siehe Abschnitt "Netzwerk Einstellungen - LAN-Parameter des iRMC S2/S3 konfigurieren" auf Seite 244 und/oder konsultieren Sie das für Ihren Server relevante Handbuch "BIOS (Aptio) Setup Utility".

► Sichern Sie die Einstellungen.

► Wenn Sie die Konsolen-Umleitung über den iRMC S2/S3 nutzen möchten, fahren Sie fort mit Abschnitt "Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren" auf Seite 50.

Wenn Sie die Text-Konsolen-Umleitung über den iRMC S2/S3 nicht nutzen möchten, beenden Sie das BIOS / TrustedCore Setup und fahren Sie fort mit dem nachfolgenden Abschnitt "LAN-Schnittstelle testen".

3.1.4 LAN-Schnittstelle testen

Für LAN-Schnittstelle können Sie wie folgt testen:

► Versuchen Sie sich über einen Web-Browser an der iRMC S2/S3-Web-Oberfläche anzumelden. Falls Sie keine Anmeldungssaufforderung erhalten, funktioniert die LAN-Schnittstelle wahrscheinlich nicht.

► Testen Sie die Verbindung zum iRMC S2/S3 mit einem Ping-Kommando.

3.2 Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren

Je nach Konfiguration der Text-Konsolen-Umleitung und Betriebssystem des Servers steht die Text-Konsolen-Umleitung zur Verfügung

– nur für die Dauer der BIOS POST-Phase oder

– über die BIOS POST-Phase hinaus auch bei laufendem Betriebssystem.

Dieser Abschnitt beschreibt:

– Konfiguration der Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore Setup Utility (für den iRMC S2).

– Konfiguration der Text-Konsolen-Umleitung via LAN über das UEFI Setup Utility (für den iRMC S3).

– Betriebssystem-spezifische Besonderheiten, die Sie beachten müssen, wenn Sie die Konsolen-Umleitung auch bei laufendem Betriebssystem nutzen wollen.

Die Text-Konsolen-Umleitung via LAN können Sie auch über die iRMC S2/S3-Web-Oberfläche konfigurieren (siehe Abschnitt "BIOS Text Konsole - Text-Konsolen-Umleitung konfigurieren und starten" auf Seite 302).

3.2.1 Text-Konsolen-Umleitung für den iRMC S2 konfigurieren

► Rufen Sie das BIOS / TrustedCore Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.

Einstellungen im Menü für die Konfiguration der Peripherie

► Rufen Sie das Menü für die Konfiguration der Peripherie auf:

Advanced – Peripheral Configuration

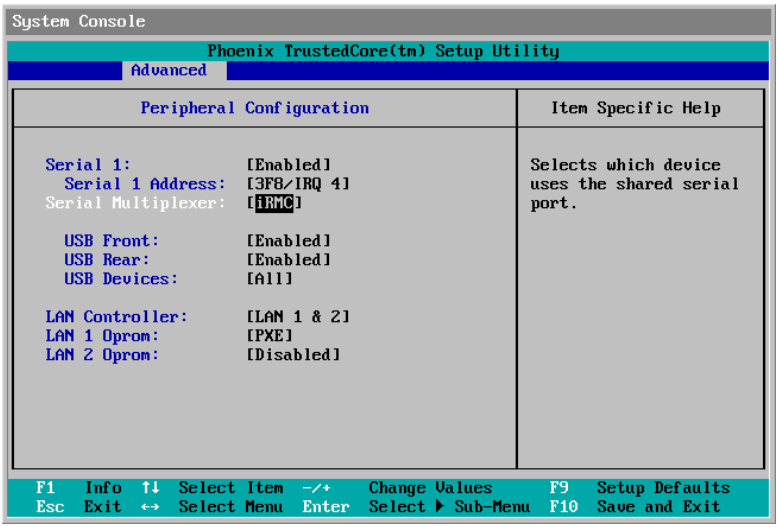

System Console
Phoenix TrustedCore(tm) Setup Utility
Advanced
Peripheral Configuration
Item Specific Help
Serial 1: [Enabled]
Serial 1 Address: [3F8/IRQ 4]
Serial Multiplexer: [iRMC]
USB Front: [Enabled]
USB Rear: [Enabled]
USB Devices: [All]
LAN Controller: [LAN 1 & 2]
LAN 1 Oprom: [PXE]
LAN 2 Oprom: [Disabled]
Selects which device uses the shared serial port.
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

Bild 10: Menü Peripheral Configuration (Darstellung im TrustedCore Setup Utility)

► Konfigurieren Sie folgende Einstellungen:

Serial 1

Setzen Sie die Einstellung auf *Enabled*.

Serial 1 Address

Akzeptieren Sie das als erstes vorgeschlagene Wertepaar.

Serial Multiplexer

Setzen Sie die Einstellung auf *iRMC*.

Einstellungen im Menü Console Redirection

► Rufen Sie das Menü *Console Redirection* auf:

Server – Console Redirection

> Das Darstellung des Menüs *Console Direction* variiert je nach verwendetem Setup Utility (BIOS oder TrustedCore).

► Konfigurieren Sie im **BIOS Setup Utility** folgende Einstellungen:

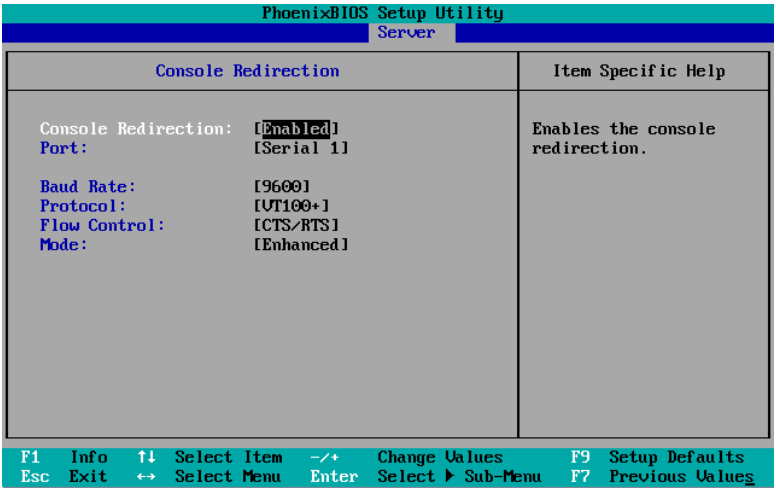

PhoenixBIOS Setup Utility
Server
Console Redirection
Item Specific Help
Console Redirection: [Enabled]
Port: [Serial 1]
Baud Rate: [9600]
Protocol: [VT100+]
Flow Control: [CTS/RTS]
Mode: [Enhanced]
Enables the console redirection.
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F7 Previous Values

Bild 11: Menü Console Redirection (Darstellung im BIOS Setup Utility)

Console Redirection
: Setzen Sie die Einstellung auf *Enabled*.

Port
: Setzen Sie die Einstellung auf *Serial 1*.

Baud Rate
: Legen Sie die Baud-Rate fest.

Protocol
: Lassen Sie diese Einstellung unverändert.(Die Einstellung hängt vom verwendeten Terminal-Typ ab.)

Flow Control
: Die Einstellung hängt vom verwendeten Teminal-Typ ab.

Mode

Diese Einstellung wirkt sich auf das Verhalten der Konsolen-Umleitung bei laufendem Betriebssystem (nach der POST-Phase) aus (siehe Abschnitt "Konsolen-Umleitung bei laufendem Betriebssystem nutzen" auf Seite 57):

Standard

Die Konsolen-Umleitung wird nach der POST-Phase des BIOS beendet.

Enhanced

Die Konsolen-Umleitung steht über die POST-Phase des BIOS hinaus zur Verfügung.

► Konfigurieren Sie im **TrustedCore Setup Utility** folgende Einstellungen:

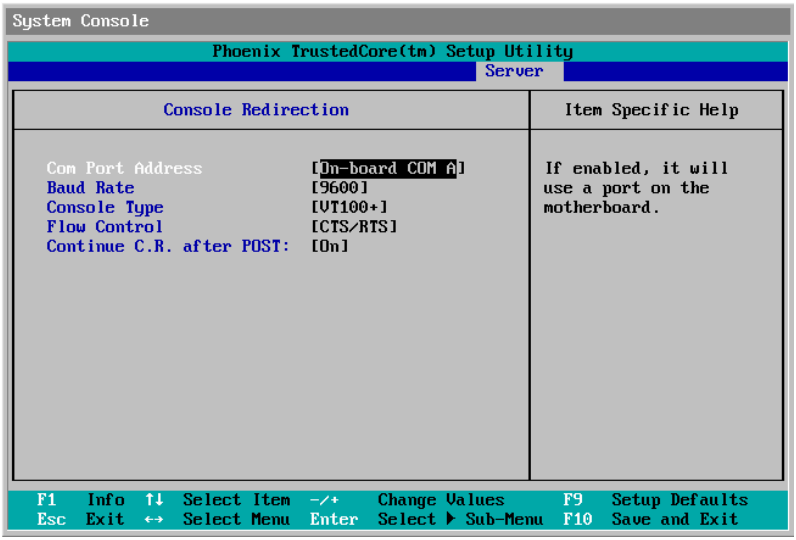

System Console
Phoenix TrustedCore(tm) Setup Utility
Server
Console Redirection
Item Specific Help
Com Port Address [On-board COM A]
Baud Rate [9600]
Console Type [VT100+]
Flow Control [CTS/RTS]
Continue C.R. after POST: [On]
If enabled, it will use a port on the motherboard.
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

Bild 12: Menü Console Redirection (Darstellung im TrustedCore Setup Utility)

Com Port Address

Setzen Sie die Einstellung auf *On-board COM A*.

Baud Rate

Legen Sie die Baud-Rate fest.

Console Type

Lassen Sie diese Einstellung unverändert.(Die Einstellung hängt vom verwendeten Terminal-Typ ab.)

Flow Control

Die Einstellung hängt vom verwendeten Teminal-Typ ab und muss am Terminal und am verwalteten Server übereinstimmen.

Continue C.R. after POST:

Diese Einstellung wirkt sich auf das Verhalten der Konsolen-Umleitung bei laufendem Betriebssystem (nach der POST-Phase) aus (siehe Abschnitt "Konsolen-Umleitung bei laufendem Betriebssystem nutzen" auf Seite 57):

Off

Die Konsolen-Umleitung wird nach der POST-Phase des BIOS beendet.

On

Die Konsolen-Umleitung steht über die POST-Phase des BIOS hinaus zur Verfügung.

BIOS / TrustedCore Setup beenden

- Sichern Sie die Einstellungen und beenden Sie das BIOS bzw. TrustedCore Setup Utility.
- Fahren Sie fort mit Abschnitt "LAN-Schnittstelle testen" auf Seite 49.

3.2.2 Text-Konsolen-Umleitung für den iRMC S3 konfigurieren

- ► Rufen Sie das UEFI Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- ► Rufen Sie das Menu *Server Mgmt* auf:

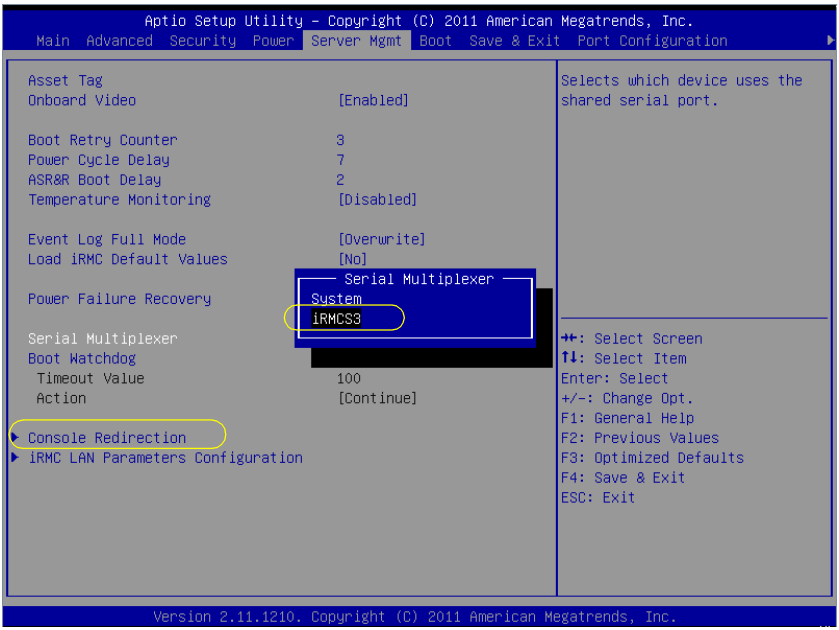


Bild 13: Menü Server Mgmt

- ► Konfigurieren Sie folgende Einstellungen:

Serial Multiplexer
Setzen Sie die Einstellung auf *iRMCS3*.

► Rufen Sie das Menü *Console Redirection* auf:

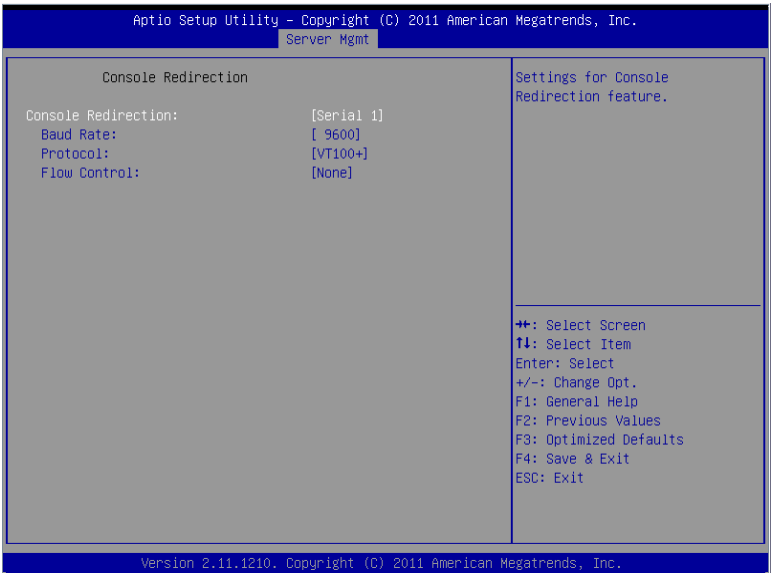


Bild 14: Menü Console Redirection

► Konfigurieren Sie im Menü *Console Redirection* folgende Einstellungen:

Console Redirection
: Setzen Sie den Wert auf *Serial 1*. Das terminal verwendet dann die erste seriell Schnittstelle.

Baud Rate
: Legen Sie die Baud-Rate fest.

Protocol
: Lassen Sie diese Einstellung unverändert. (Die Einstellung hängt vom verwendeten Terminal-Typ ab.)

Flow Control
: Die Einstellung hängt vom verwendeten Teminal-Typ ab und muss am Terminal und am verwalteten Server übereinstimmen.

UEFI Setup beenden

► Sichern Sie die Einstellungen und beenden Sie das BUEFI Setup Utility.

► Fahren Sie fort mit Abschnitt "LAN-Schnittstelle testen" auf Seite 49.

3.2.3 Konsolen-Umleitung bei laufendem Betriebssystem nutzen

Sie können - je nach Betriebssystem des verwalteten Servers - auch nach der BIOS POST-Phase noch die Konsolen-Umleitung nutzen.

DOS

Die BIOS-Einstellung für den Modus der Konsolen-Umleitung muss wie folgt konfiguriert sein (siehe Abschnitt "Einstellungen im Menü Console Redirection" auf Seite 52):

– BIOS Setup Utility: *Mode: Enhanced*

– TrustedCore Setup Utility: *Continue C.R. after POST: On*

Windows Server 2003 / 2008

Wenn die Konsolen-Umleitung bereits während der Windows-Installation aktiviert wird, wird Sie im Rahmen der Windows-Installation automatisch konfiguriert.

Wenn die Konsolen-Umleitung erst nach Abschluss der Windows-Installation aktiviert wird, muss sie „von Hand“ konfiguriert werden.

Windows Server 2003 / 2008 übernimmt nach der POST-Phase automatisch die Konsolen-Umleitung, ohne dass weitere Einstellungen notwendig sind. Während der Boot-Phase des Betriebssystems wird die SAC-Konsole von Windows Server 2003 übertragen:

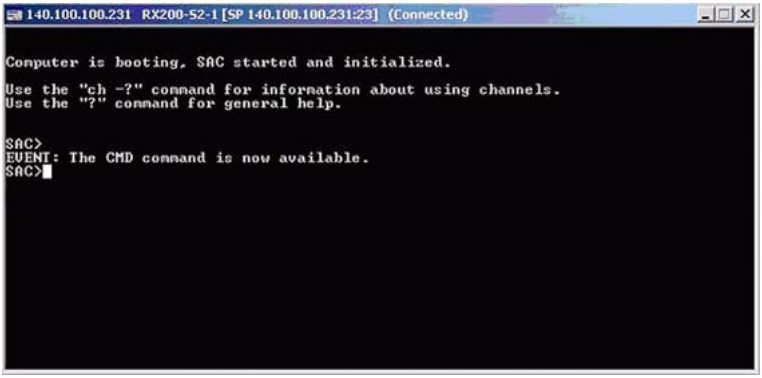

140.100.100.231 RX200-S2-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: The CMD command is now available.
SAC>

Bild 15: SAC-Konsole von Windows Server 2003

Linux

Ein Linux-Betriebssystem müssen Sie konfigurieren, damit es die Konsolen-Umleitung nach der POST-Phase übernimmt. Wenn es konfiguriert ist, haben Sie vom Remote-Arbeitplatz aus vollen Zugriff.

Notwendige Einstellungen

Die Einstellungen können sich je nach Programmversion etwas ändern.

SuSe und RedHat

Fügen Sie am Ende der Datei */etc/inittab* folgende Zeile an:

```
xx:12345:respawn:/sbin/agetty <baudrate> ttyS0
```

RedHat

Fügen Sie in die Datei */etc/grub.conf* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

SuSE

Fügen Sie in die Datei */boot/grub/menu.lst* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

3.3 Serielle Schnittstelle des iRMC S2/S3 konfigurieren und nutzen

Die serielle Schnittstelle des iRMC S2/S3 bietet Ihnen folgende Möglichkeiten:

– Über Nullmodem-Kabel können Sie die Terminal-Anwendung Remote Manager (Serial) nutzen (siehe Abschnitt "Benutzeroberfläche Remote Manager (Serial) nutzen" auf Seite 65).

– **Nur für den iRMC S2:** Weiterleitung von Alarmen über Modem (Alerting). Das Alerting via Modem können Sie über die Web-Oberfläche des iRMC S2 konfigurieren (siehe Abschnitt "Serielle / Modem Benachrichtigungen - Alarmweiterleitung über Modem konfigurieren" auf Seite 263).

3.3.1 Die serielle Schnittstelle des iRMC S2 konfigurieren

- Rufen Sie das BIOS bzw. TrustedCore Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- Rufen Sie das Menü *Peripheral Configuration* auf, um den seriellen Port zu konfigurieren:

  Advanced – Peripheral Configuration

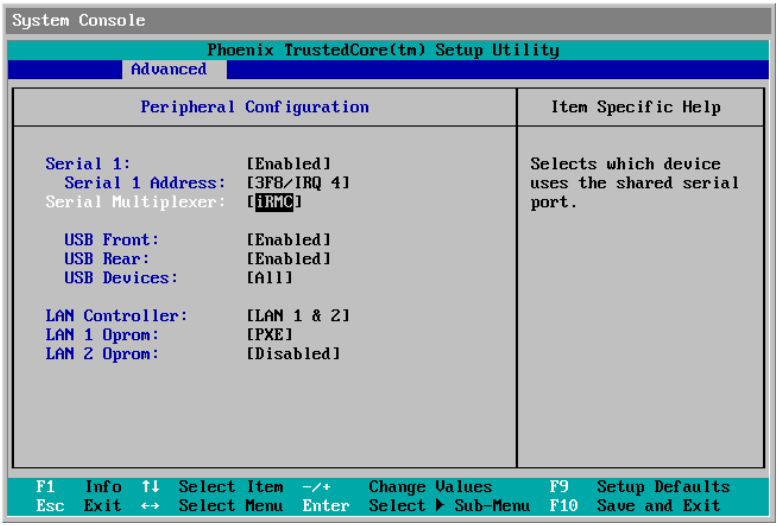

System Console
Phoenix TrustedCore(tm) Setup Utility
Advanced
Peripheral Configuration
Item Specific Help
Serial 1: [Enabled]
Serial 1 Address: [3F8/IRQ 4]
Serial Multiplexer: [iRMC]
USB Front: [Enabled]
USB Rear: [Enabled]
USB Devices: [All]
LAN Controller: [LAN 1 & 2]
LAN 1 Oprom: [PXE]
LAN 2 Oprom: [Disabled]
Selects which device uses the shared serial port.
F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

Bild 16: Menü Peripheral Configuration (Darstellung im TrustedCore Setup Utility)

- Konfigurieren Sie folgende Einstellung:

  Serial 1

  Setzen Sie die Einstellung auf *Enabled*.

  Serial 1 Address

  Akzeptieren Sie das als erstes vorgeschlagene Wertepaar.

  Serial Multiplexer

  Setzen Sie die Einstellung auf *iRMC*.

Die folgenden, im Menü nicht angezeigten Werte sind voreingestellt (siehe Seite 65, "Terminalprogramm (VT100+)"):

Bits per second
9600

Data bits
8

Parity
None.

Stop bits
1

Flow Control
None

BIOS / TrustedCore Setup beenden

- Sichern Sie die Einstellungen und beenden Sie das BIOS bzw. TrustedCore Setup Utility.
- Fahren Sie fort mit Abschnitt "LAN-Schnittstelle testen" auf Seite 49.

3.3.2 Die serielle Schnittstelle des iRMC S3 konfigurieren

- ► Rufen Sie das UEFI Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- ► Rufen Sie das Menü *Server Mgmt* auf:

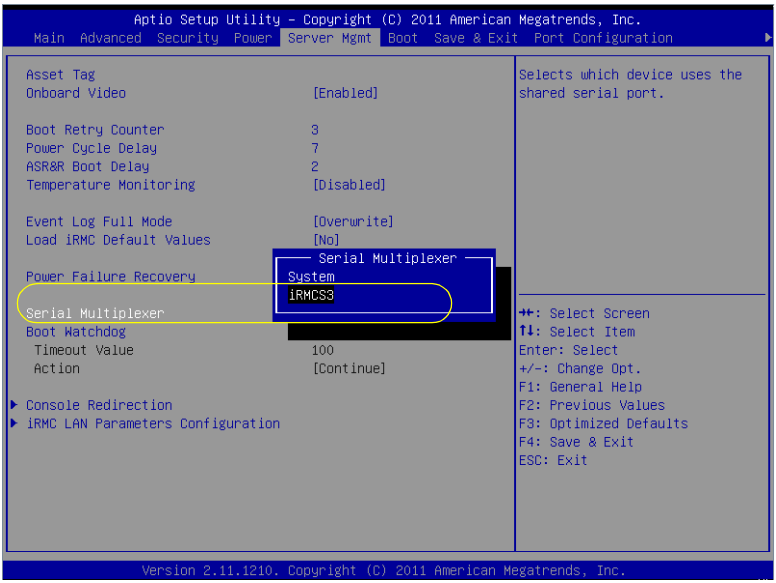


Bild 17: Menü Server Mgmt

- ► Konfigurieren Sie die folgenden Einstellungen:

Serial Multiplexer

Setzen Sie die Einstellung aus *iRMCS3*.

► Rufen Sie da Menü *Serial Port 1 Configuration* auf, um den seriellen Port zu konfigurieren:

Advanced – Super IO Configuration – Serial Port 1 Configuration.

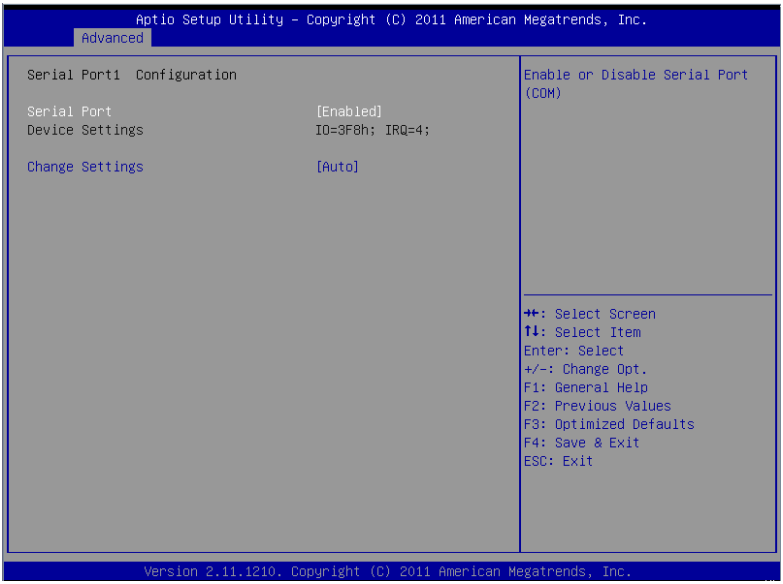


Bild 18: Menü Serial Port 1 Configuration

► Konfigurieren Sie folgende Einstellungen:

Serial Port

Setzen Sie die Einstellung auf *Enabled*.

Device Settings

Zeigt die Ein-/Ausgabe-Adresse und den Interrupt für den zugehörigen seriellen Port , z.B. IO=3F8h; IRQ=4.

Akzeptieren Sie den vorgeschlagenen Wert.

Die folgenden, im Menü nicht angezeigten Werte sind voreingestellt (siehe Seite 65, "Terminalprogramm (VT100+)")

Bits per second

9600

Data bits

8

Parity
None.

Stop bits
1

Flow Control
None

UEFI Setup beenden

- Sichern Sie die Einstellungen und beenden Sie das UEFI Setup Utility.
- Fahren Sie fort mit Abschnitt "LAN-Schnittstelle testen" auf Seite 49.

3.3.3 Benutzeroberfläche Remote Manager (Serial) nutzen

Wenn Sie über eine Nullmodemkabel einen Rechner anschließen und auf diesem Rechner ein Terminalprogramm (VT100+) starten, können Sie auf die Terminal-Anwendung Remote Manager (Serial) zugreifen. Die Oberfläche des Remote Manager (Serial) ist identisch mit der Oberfläche des Remote Manager (siehe Kapitel "iRMC S2/S3 über Telnet/SSH (Remote Manager)" auf Seite 333).

Voraussetzungen

Am verwalteten Server:

Die BIOS-Einstellung *Serial Multiplexer* muss auf *iRMC* konfiguriert sein (siehe Abschnitt "Die serielle Schnittstelle des iRMC S2 konfigurieren" auf Seite 60).

Terminalprogramm (VT100+):

Konfigurieren Sie für das Terminalprogramm folgende Port-Einstellungen:

Bits per second
: Setzen Sie die Einstellung auf *9600*.

Data bits
: Setzen Sie die Einstellung auf *8*.

Parity
: Setzen Sie die Einstellung auf *None*.

Stop bits
: Setzen Sie die Einstellung auf *1*.

Flow Control
: Setzen Sie die Einstellung auf *None*.

3.4 iRMC S2/S3 über die iRMC S2/S3-Web-Oberfläche konfigurieren

► Starten Sie die iRMC S2/S3-Web-Oberfläche (siehe Abschnitt "An der iRMC S2/S3-Web-Oberfläche anmelden" auf Seite 142).

3.4.1 LAN-Parameter konfigurieren

► Wählen Sie im Navigationsbereich den Eintrag *Netzwerk Einstellungen* (siehe Abschnitt "Netzwerk Einstellungen - LAN-Parameter des iRMC S2/S3 konfigurieren" auf Seite 244).

LAN-Einstellungen konfigurieren

► Konfigurieren Sie die LAN-Einstellungen auf der Seite *Netzwerk Schnittstelle*. Für die erforderlichen Einstellungen siehe Abschnitt "Netzwerk Schnittstelle-Ethernet-Einstellungen des iRMC S2/S3 konfigurieren" auf Seite 245.

Ports und Netzwerk-Dienste konfigurieren

► Konfigurieren Sie die Ports und Netzwerk-Dienste in der Seite *Ports und Netzwerk Dienste*. Für die erforderlichen Einstellungen siehe Abschnitt "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 252.

DHCP/DNS (Dynamic DNS) konfigurieren

► Konfigurieren Sie die DHCP- und DNS-Einstellungen in der Seite *DNS Konfiguration*. Für die erforderlichen Einstellungen siehe Abschnitt "DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren" auf Seite 256.

3.4.2 Alarmbenachrichtigung (Alerting) konfigurieren

Die Seiten für die Konfiguration der Alarmbenachrichtigung sind im Navigationsbereich unter *Benachrichtigungen* zusammengefasst (siehe Abschnitt "Benachrichtigungen - Alarmbenachrichtigung konfigurieren" auf Seite 260).

Weiterleitung von Alarmen über SNMP konfigurieren

- Klicken Sie im Navigationsbereich auf *SNMP Traps*. Die Seite *SNMP Trap Benachrichtigung* wird angezeigt.
- Konfigurieren Sie die Weiterleitung von SNMP Traps. Für die erforderlichen Einstellungen siehe Abschnitt "SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren" auf Seite 261.

Weiterleitung von Alarmen über Modem an Mobiltelefon konfigurieren (nur bei iRMC S2)

- Klicken Sie im Navigationsbereich auf *Seriell/Modem*. Die Seite *Serielle / Modem Benachrichtigung* wird angezeigt.
- Konfigurieren Sie die Weiterleitung von Alarmen über Modem. Für die erforderlichen Einstellungen siehe Abschnitt "Serielle / Modem Benachrichtigungen - Alarmweiterleitung über Modem konfigurieren" auf Seite 263.

E-Mail-Benachrichtigung (Email Alerting) konfigurieren

- Klicken Sie im Navigationsbereich auf *E-Mail*. Die Seite *E-Mail Benachrichtigung* wird angezeigt.
- Konfigurieren Sie die E-Mail-Benachrichtigung. Für die erforderlichen Einstellungen siehe Abschnitt "E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren" auf Seite 265.

3.4.3 Text-Konsolen-Umleitung konfigurieren

- Konfigurieren Sie die Umleitung der Text-Konsole im Fenster *BIOS Text Konsole*. Für die erforderlichen Einstellungen siehe Abschnitt "BIOS Text Konsole - Text-Konsolen-Umleitung konfigurieren und starten" auf Seite 302.

4 Benutzerverwaltung für den iRMC S2/S3

Die Benutzerverwaltung für den iRMC S2/S3 verwendet zwei verschiedene Arten von Benutzerkennungen:

– **Lokale Benutzerkennungen** sind lokal im nicht-flüchtigen Speicher des iRMC S2/S3 hinterlegt und werden über die Benutzerschnittstellen des iRMC S2/S3 verwaltet.

– **Globale Benutzerkennungen** sind in der zentralen Datenhaltung eines Verzeichnisdienstes (Directory Service) hinterlegt und werden über die Schnittstellen dieses Verzeichnisdienstes verwaltet.

  Für die globale iRMC S2/S3-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDS

Das vorliegende Kapitel informiert über folgende Themen:

– Konzept der Benutzerverwaltung für den iRMC S2/S3
– Benutzerberechtigungen
– lokale Benutzerverwaltung am iRMC S2/S3

Detaillierte Informationen zur globalen Benutzerverwaltung für den iRMC S2/S3 mithilfe der einzelnen Verzeichnisdienste finden Sie im Handbuch „Benutzerverwaltung in ServerView“.

4.1 Konzept der Benutzerverwaltung für den iRMC S2/S3

Die Benutzerverwaltung für den iRMC S2/S3 unterstützt die parallele Verwaltung lokaler und globaler Benutzerkennungen.

Bei der Validierung der Authentisierungsdaten (Benutzername, Passwort), die ein Benutzer beim Login an einer der iRMC S2/S3-Schnittstellen eingibt, verfährt der iRMC S2/S3 gemäß dem folgenden Ablauf (siehe auch Bild 19 auf Seite 71):

1. Der iRMC S2/S3 gleicht den Benutzernamen und das Passwort mit den lokal gespeicherten Benutzerkennungen ab:
   - Bei erfolgreicher Authentifizierung des Benutzers durch den iRMC S2/S3 (Benutzername und Passwort sind gültig) darf sich der Benutzer einloggen.
   - Andernfalls setzt der iRMC S2/S3 die Prüfung mit Schritt 2. fort.
2. Der iRMC S2/S3 authentisiert sich beim Verzeichnisdienst via LDAP mit Benutzernamen und Passwort, ermittelt per LDAP-Anfrage die Benutzerrechte und prüft, ob der Benutzer damit am iRMC S2/S3 arbeiten darf.

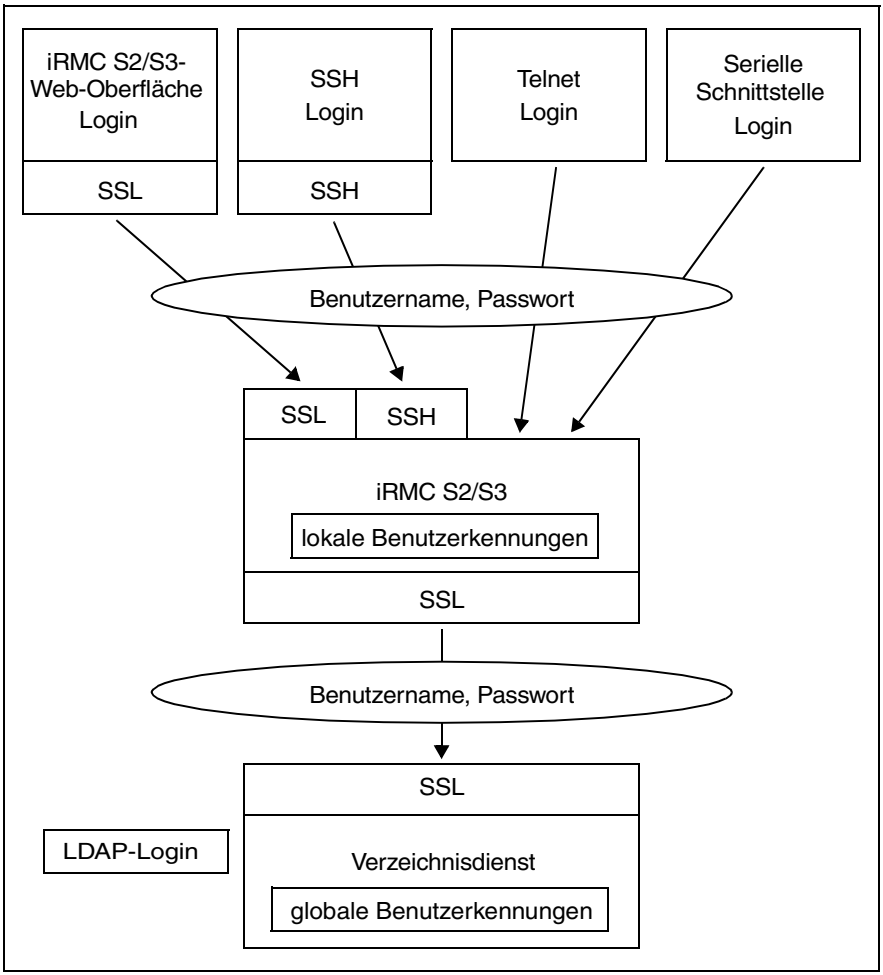


Bild 19: Login-Authentifizierung durch den iRMC S2/S3

Die Nutzung von SSL für die LDAP-Verbindung zwischen dem iRMC S2/S3 und dem Verzeichnisdienst ist optional, wird jedoch empfohlen. Eine SSL-gesicherte LDAP-Verbindung zwischen iRMC S2/S3 und Verzeichnisdienst garantiert den sicheren Austausch der Daten, insbesondere auch von Benutzernamen und Passwort.

SSL-Login über die iRMC S2/S3-Web-Oberfläche ist nur dann erforderlich, wenn LDAP aktiviert ist (Option *LDAP enable*, siehe Seite 283).

4.2 Benutzerberechtigungen

Der iRMC S2/S3 unterscheidet zwei verschiedene Arten von Benutzerberechtigungen, die sich ergänzen:

– Kanal-spezifische Privilegien (via Zuordnung zu Kanal-spezifischen Berechtigungsgruppen)

– Berechtigungen zur Nutzung spezieller iRMC S2/S3-Funktionen

Welche dieser Privilegien und Berechtigungen zur Nutzung der einzelnen iRMC S2/S3-Funktionen erforderlich sind, ist beschrieben

– für die iRMC S2/S3-Web-Oberfläche auf Seite 144,

– für den Remote Manager auf Seite 342.

– für das Server Management Tool (IPMIVIEW) im Handbuch „IPMIVIEW“.

Kanal-spezifische Privilegien (Kanal-spezifische Berechtigungsgruppen)

Der iRMC S2/S3 ordnet jede Benutzerkennung einer der folgenden vier Kanal-spezifischen Berechtigungsgruppen zu:

– Benutzer
– Operator
– Administrator
– OEM

Da der iRMC S2/S3 diese Berechtigungen Kanal-spezifisch erteilt, kann ein Benutzer verschiedene Rechte haben, je nachdem, ob er auf den iRMC S2/S3 über die LAN-Schnittstelle oder über die serielle Schnittstelle zugreift.

Der Berechtigungsumfang nimmt beginnend bei *Benutzer* (niedrigste Berechtigungsstufe) über *Operator* und *Administrator* bis *OEM* (höchste Berechtigungsstufe) stetig zu.

Die Berechtigungsgruppen entsprechen dem IPMI Privilege Level. Bestimmte Rechte (z.B. für das Power Management) sind an diese Gruppen bzw. Privilege Level gebunden.

Berechtigungen zur Nutzung spezieller iRMC S2/S3-Funktionen

Zusätzlich zu den Kanal-spezifischen Berechtigungen können Sie einem Benutzer individuell folgende Berechtigungen erteilen:

- **Benutzer konfigurieren erlaubt**
  Berechtigung zum Konfigurieren von lokalen Benutzerkennungen
- **iRMC S2/S3 Einstellungen konfigurieren**
  Berechtigung zum Konfigurieren der iRMC S2/S3-Einstellungen
- **Konsolen Umleitung erlaubt**
  Berechtigung zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection) im „Nur Lesen“- und „Volle Kontrolle“- Modus
- **Remote Storage erlaubt**
  Berechtigung zur Nutzung der Remote Storage-Funktionalität

Vorkonfigurierte Benutzerkennung

Die Firmware des iRMC S2/S3 stellt eine Standard-Administratorkennung für den iRMC S2/S3 zur Verfügung, die sämtliche Berechtigungen besitzt:

Administratorkennung: admin

Kennwort: admin

Für Administratorkennung und Kennwort wird bei lokalen Benutzern zwischen Groß- und Kleinschreibung unterschieden.

Es wird dringend empfohlen, nach der Anmeldung möglichst bald eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort der Kennung zu ändern (siehe Abschnitt "Benutzerverwaltung" auf Seite 272).

4.3 Lokale Benutzerverwaltung für den iRMC S2/S3

Der iRMC S2/S3 verfügt über eine eigene lokale Benutzerverwaltung. Es können bis zu 16 Benutzer mit Kennwörtern konfiguriert und je nach Gruppenzugehörigkeit mit unterschiedlichen Rechten ausgestattet werden. Die Benutzerkennungen werden im lokalen, nicht-flüchtigen Speicher des iRMC S2/S3 abgelegt.

Für die Benutzerverwaltung am iRMC S2/S3 stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Benutzerverwaltung über die Web-Oberfläche

– Benutzerverwaltung über den Server Configuration Manager

4.3.1 Lokale Benutzerverwaltung über die iRMC S2/S3-Web-Oberfläche

Die Benutzerverwaltung am iRMC S2/S3 erfordert *Benutzer konfigurieren erlaubt*-Berechtigung.

An der Web-Oberfläche können Sie sich die Liste der konfigurierten Benutzer anzeigen lassen. Außerdem können Sie neue Benutzer konfigurieren, die Konfiguration bereits existierender Benutzer ändern sowie Benutzer aus der Liste entfernen.

► Starten Sie die iRMC S2/S3-Web-Oberfläche (siehe Abschnitt "An der iRMC S2/S3-Web-Oberfläche anmelden" auf Seite 142).

Liste der konfigurierten Benutzer anzeigen

► Klicken Sie im Navigationsbereich auf den die Funktion *Benutzerverwaltung - iRMC S2/S3 Benutzer*.

Die Seite *Benutzer Verwaltung* mit der Liste der konfigurierten Benutzer öffnet sich (siehe Seite 273). Dort können Sie Benutzer löschen sowie die Seite für die Konfiguration neuer Benutzer aufrufen.
Die Beschreibung zu dieser Seite finden Sie im Abschnitt "Benutzerverwaltung" auf Seite 272.

Neuen Benutzer konfigurieren

- Klicken Sie in der Seite *Benutzer Verwaltung* auf die Schaltfläche *Neuer Benutzer.*

  Die Seite *Neuen Benutzer konfigurieren* öffnet sich. In dieser Seite können Sie die Grundeinstellungen des neuen Benutzers konfigurieren. Die Beschreibung zu dieser Seite finden Sie im Abschnitt "Neuen Benutzer konfigurieren" auf Seite 274.

Konfiguration eines Benutzers ändern

- Klicken Sie in der Seite *Benutzer Verwaltung* auf den Namen des Benutzers, dessen Konfigurationsparameter Sie ändern wollen.

  Die Seite *Benutzer '<name>' Konfiguration* öffnet sich mit den Einstellungen des ausgewählten Benutzers. Dort können Sie die Konfigurationsparameter des neuen Benutzers ändern. Die Beschreibung zu dieser Seite finden Sie im Abschnitt "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 275.

Benutzer löschen

- Klicken Sie in der Seite *Benutzer Verwaltung* auf die Schaltfläche *Löschen*, die sich in der Zeile des zu löschenden Benutzers befindet.

4.3.2 Lokale Benutzerverwaltung über den Server Configuration Manager

Voraussetzung:

Auf dem verwalteten Server sind die aktuellen ServerView-Agenten installiert.

Die Benutzerverwaltung am iRMC S2/S3 erfordert *Benutzer konfigurieren erlaubt (Configure User Accounts)*-Berechtigung.

Die Benutzerverwaltung mit dem Server Configuration Manager entspricht weitgehend der Benutzerverwaltung via iRMC S2/S3-Web-Oberfläche.

Im Kapitel "iRMC S2/S3 via Server Configuration Manager konfigurieren" auf Seite 359 ist beschrieben, wie Sie den Server Configuration Manager starten. Näheres zu den einzelnen Dialogen des Server Configuration Managers finden Sie in der Online-Hilfe des Server Configuration Managers.

4.3.3 SSHv2 Public Key-Authentifizierung für lokale iRMC S2/S3-Benutzer

Neben der Authentisierung mit Benutzername und Passwort unterstützt der iRMC S2/S3 für lokale Benutzer zusätzlich die SSHv2-basierte Public Key-Authentisierung mithilfe von Paaren aus öffentlichem und privatem Schlüssel. Für die SSHv2 Public Key-Authentifizierung wird der öffentliche SSHv2-Schlüssel eines iRMC S2/S3-Benutzers auf den iRMC S2/S3 geladen, während der iRMC S2/S3-Benutzer seinen privaten Schlüssel z.B. über das Programm *PuTTY* oder das OpenSSH Client-Programm *ssh* verwendet.

Der iRMC S2/S3 unterstützt die folgenden Typen öffentlicher Schlüssel:

– SSH DSS (mindestens erforderlich)
– SSH RSA (empfohlen)

Die öffentlichen SSHv2-Schlüssel (SSHv2 Public Keys), die Sie auf den iRMC S2/S3 laden, können wahlweise in einem Format gemäß RFC4716 oder im OpenSSH-Format vorliegen (siehe Seite 278).

Public Key-Authentifizierung

In groben Zügen stellt sich Public Key-Authentifizierung eines Benutzers am iRMC S2/S3 wir folgt dar:

Der Benutzer, der sich am iRMC S2/S3 anmelden will, erzeugt das Schlüsselpaar:

– Der private Schlüssel bleibt lesegeschützt auf dem Computer des Benutzers.

– Den öffentlichen Schlüssel lädt der Benutzer (oder der Administrator) auf den iRMC S2/S3.

Bei entsprechender Konfiguration kann sich der Benutzer nun ohne Passwort und sehr sicher an diesem iRMC S2/S3 anmelden. Der Benutzer ist lediglich für die Geheimhaltung seines privaten Schlüssels verantwortlich.

Im Einzelnen umfasst die Einrichtung einer Public Key-Authentifizierung folgende Schritte, die in den nachfolgenden Abschnitten näher erläutert sind:

1. Öffentlichen und privaten SSHv2-Schlüssel mit dem Programm *PuTTYgen* oder *ssh-keygen* erzeugen und in separate Dateien sichern (siehe Seite 78).
2. Öffentlichen SSHv2-Schlüssel aus Datei auf den iRMC S2/S3 laden (siehe Seite 82).
3. Das Programm *PuTTY* bzw. *ssh* für den SSHv2-Zugriff auf den iRMC S2/S3 konfigurieren (siehe Seite 84).

4.3.3.1 Öffentlichen und privaten SSHv2-Schlüssel erzeugen

Den öffentlichen und den privatenSSHv2-Schlüssel erzeugen Sie wahlweise

– mit dem Programm *PuTTYgen* oder

– mit dem OpenSSH-Client-Programm *ssh-keygen*.

Öffentlichen und privaten SSHv2-Schlüssel mit PuTTYgen erzeugen

Gehen Sie wie folgt vor:

► Starten Sie *PuTTYgen* auf Ihrem Windows-Rechner

Nach dem Start meldet sich *PuTTYgen* mit dem folgenden Fenster:

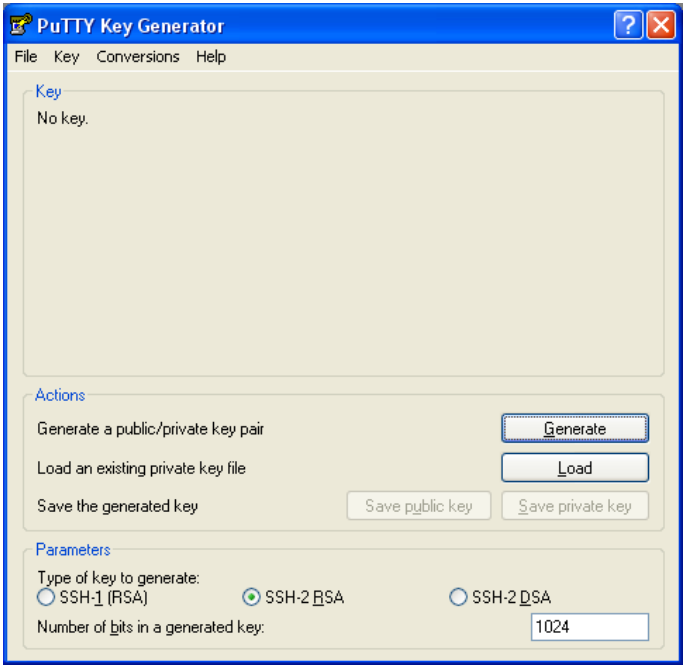


Bild 20: PuTTYgen: Neuen privaten und öffentlichen SSHv2-Schlüssel erzeugen

► Wählen Sie unter *Parameters* den Schlüsseltyp *SSH-2RSA* und klicken Sie auf *Generate*, um die Schlüsselgenerierung zu starten.

Danach wird unter *Key* der Generierungsfortschritt angezeigt (siehe Bild 21 auf Seite 79).

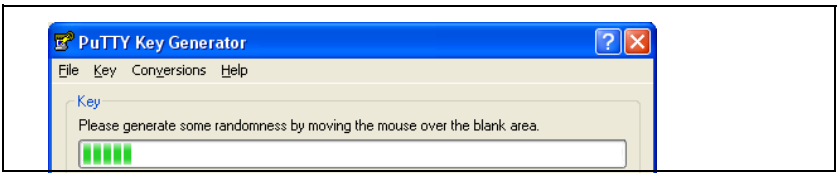

PuTTY Key Generator
File Key Conversions Help
Key
Please generate some randomness by moving the mouse over the blank area.

Bild 21: PuTTYgen: Neues Schlüsselpaar erzeugen (Fortschrittsanzeige).

► Bewegen Sie den Mauszeiger über die freie Fläche der Fortschrittsanzeige, um die Zufälligkeit der generierten Schlüssel zu erhöhen.

Nach Abschluss der Schlüsselgenerierung zeigt *PuTTYgen* Schlüssel und Fingerprint des öffentlichen SSHv2-Schlüssels an:

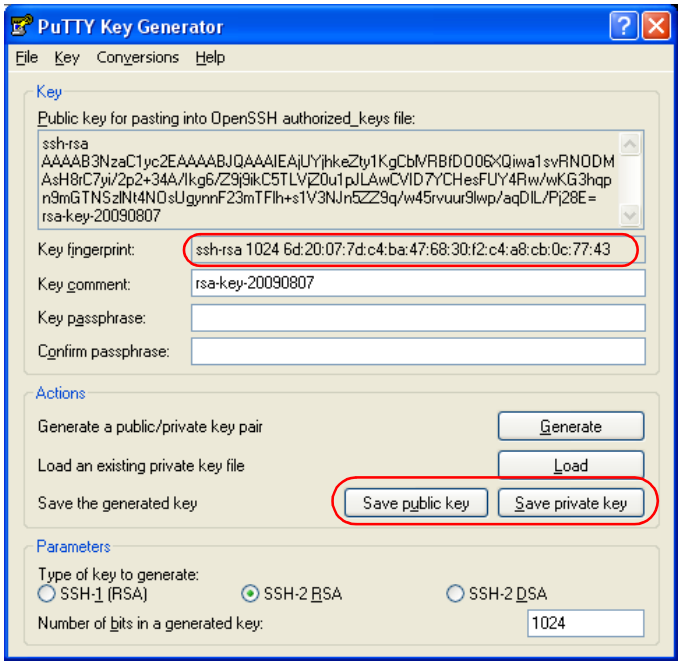


Bild 22: PuTTYgen: Neuen privaten SSHv2-Schlüssel erzeugen (Fortschrittsanzeige).

► Klicken Sie auf *Save public key*, um den öffentlichen SSHv2-Schlüssel in eine Datei zu speichern. Aus dieser Datei können Sie den öffentlichen Schlüssel auf den iRMC S2/S3 hochladen (siehe Seite 82).

► Klicken Sie auf *Save private key*, um den privaten SSHv2-Schlüssel für die Verwendung mit *PuTTY* (siehe Seite 84) in eine Datei zu speichern.

Öffentlichen und privaten SSHv2-Schlüssel mit ssh-keygen erzeugen

Sofern OpenSSH in der von Ihnen verwendeten Linux-Distribution nicht bereits installiert ist, können Sie OpenSSH von *http://www.openssh.org* beziehen.

Die ausführliche Beschreibung der Operanden finden Sie auf den Man Pages von OpenSSH unter *http://www.openssh.org/manual.html*

Gehen Sie wie folgt vor:

- Rufen Sie *ssh-keygen* für die Generierung eines RSA-Schlüsselpaars auf:

  ```
  ssh-keygen -t rsa
  ```

  ssh-keygen protokolliert den Ablauf der Schlüsselgenerierung. Dabei fragt *ssh-keygen* nach dem Dateinamen, unter dem der private Schlüssel abgespeichert werden soll, sowie nach einer Passphrase für den privaten Schlüssel. Als Ergebnis speichert privaten und öffentlichen SSHv2-Schlüssel in separaten Dateien ab und zeigt den Fingerprint des öffentlichen Schlüssels an.

Beispiel: RSA-Schlüsselpaar mit ssh -keygen generieren

```
$HOME/benutzer1 ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key
($HOME/benutzer1/.ssh/id_rsa):                                  1
Enter passphrase (empty for no passphrase):                     2
Enter same passphrase again:
Your identification has been saved in
$HOME/benutzer1/.ssh/id_rsa.                                    3
Your public key has been saved in
$HOME/benutzer1/.ssh/id_rsa.pub.                                4
The key fingerprint is:
ee:99:d7:ac:8f:8e:c7:2f:2c:9b:81:80:3f:84:28:7d                 5
                                  benutzer1@mycomp
```

Erläuterung:

1. *ssh-keygen* fragt nach dem Dateinamen, unter dem der private SSHv2-Schlüssel abgespeichert werden soll. Wenn Sie ohne Eingabe eines Dateinamens mit Enter bestätigen, verwendet *ssh-keygen* den Standard-Dateinamen *id_rsa*.
2. *ssh-keygen* fordert Sie auf, eine Passphrase (inklusive Bestätigung) zur Verschlüsselung des privaten Schlüssels einzugeben. Wenn Sie ohne Eingabe einer Passphrase mit Enter bestätigen, verwendet *ssh-keygen* keine Passphrase.
3. *ssh-keygen* informiert, dass der neu generierte private SSHv2-Schlüssel in der Datei */.ssh/id_rsa* gespeichert wurde.
4. *ssh-keygen* informiert, dass der neu generierte öffentliche SSHv2-Schlüssel in der */.ssh/id_rsa.pub* gespeichert wurde.
5. *ssh-keygen* zeigt Fingerprint des öffentlichen SSHv2-Schlüssels sowie die lokale Benutzkennung, zu der der öffentliche Schlüssel gehört.

4.3.3.2 Öffentlichen SSHv2-Schlüssel aus Datei auf den iRMC S2/S3 laden.

Gehen Sie wie folgt vor:

► Öffnen Sie in der iRMC S2/S3 Web-Oberfläche über die Seite *iRMC S2 Benutzer Verwaltung* die Detailansicht für den gewünschten Benutzer (hier: *user3*):

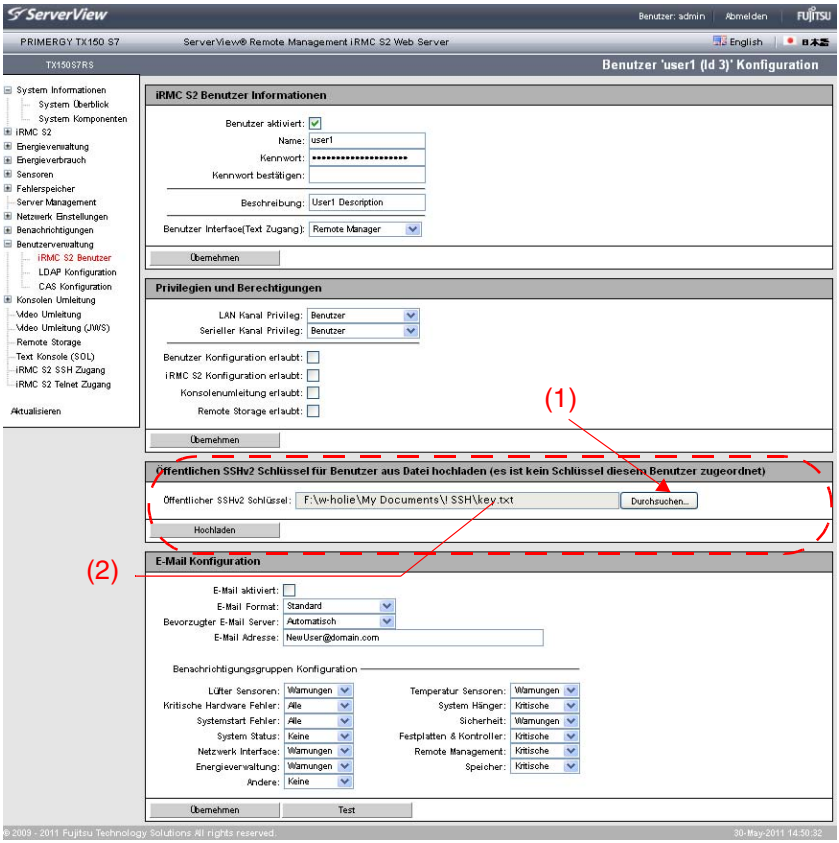


Bild 23: iRMC S2/S3 Web-Oberfläche: Öffentlichen SSHv2 Schlüssel auf den iRMC S2/S3 laden

► Klicken Sie in der Gruppe *Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen* auf *Durchsuchen* (1), und navigieren Sie zu der Datei, die den gewünschten öffentlichen Schlüssel enthält (2).

► Klicken Sie auf *Hochladen*, um den öffentlichen Schlüssel auf den iRMC S2/S3 zu laden.

Nach erfolgreichem Hochladen zeigt der iRMC S2/S3 den Key Fingerprint in der Gruppe *Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen* an:

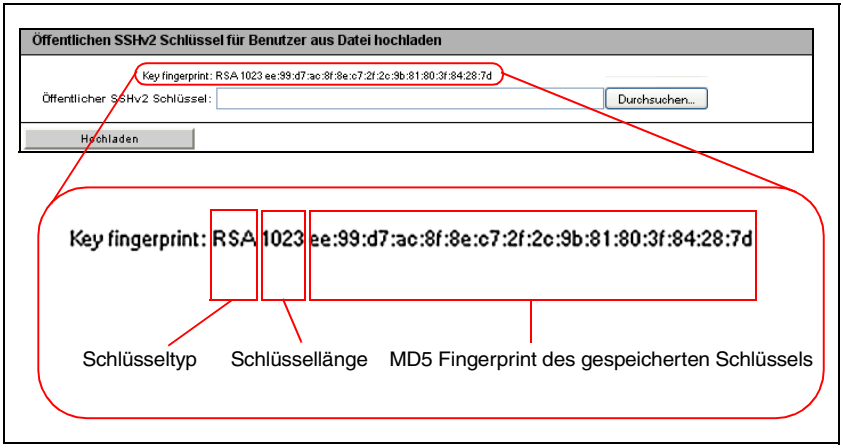


Bild 24: Anzeige des Key fingerprint

Vergewissern Sie sich aus Sicherheitsgründen, dass der hier angezeigte Fingerprint mit dem in *PuTTYgen* (siehe Bild 22 auf Seite 79) unter *Key fingerprint* angezeigten Fingerprint übereinstimmt.

4.3.3.3 PuTTY und OpenSSH Client für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren

PuTTY für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren

Mithilfe des Programms *PuTTY* können eine Public Key-authentifizierte Verbindung zum iRMC S2/S3 herstellen und sich dort wahlweise unter Ihrem Benutzernamen oder via Auto-Login anmelden. Dabei wickelt *PuTTY* das Authentifizierungsprotokoll automatisch auf Basis des zuvor erzeugten Paars aus privatem und öffentlichem SSHv2-Schlüssel ab.

Gehen Sie wie folgt vor:

- Starten Sie *PuTTY* auf Ihrem Windows Computer.

  Nach dem Start meldet sich *PuTTY* mit dem folgenden Fenster:

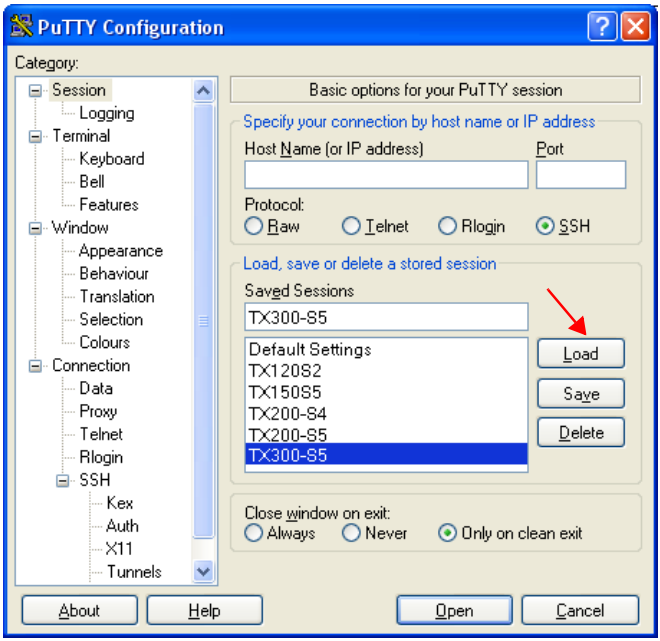


Bild 25: PuTTY: SSH-Sitzung auswählen und laden

- Wählen Sie eine gespeicherte SSH-Sitzung oder erzeugen Sie eine neue SSH-Sitzung für den iRMC S2/S3, mit dem Sie den öffentlichen SSHv2-Schlüssel verwenden wollen.

► Klicken Sie auf *Load*, um die gewählte SSH-Sitzung zu laden.

Das folgende Fenster wird angezeigt:

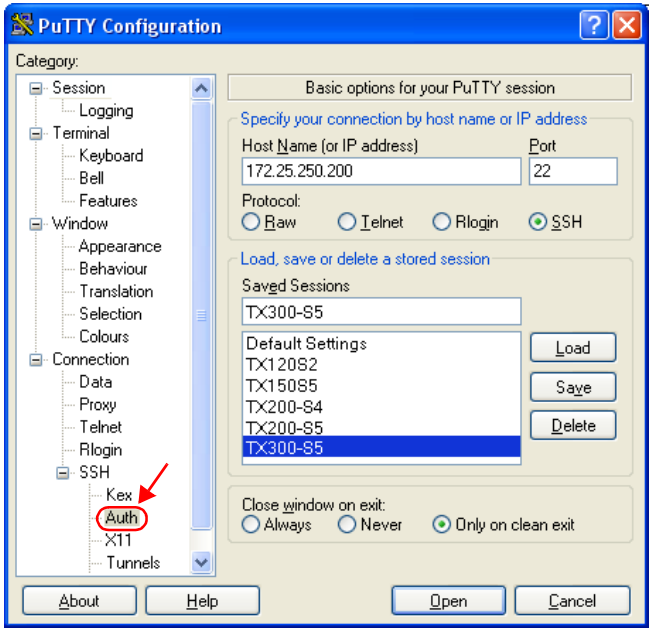


Bild 26: PuTTY: SSH-Sitzung geladen

► Wählen Sie *SSH - Auth*, um die Optionen für die SSH-Authentifizierung zu konfigurieren.

Das folgende Fenster wird angezeigt (siehe Bild 27 auf Seite 86).

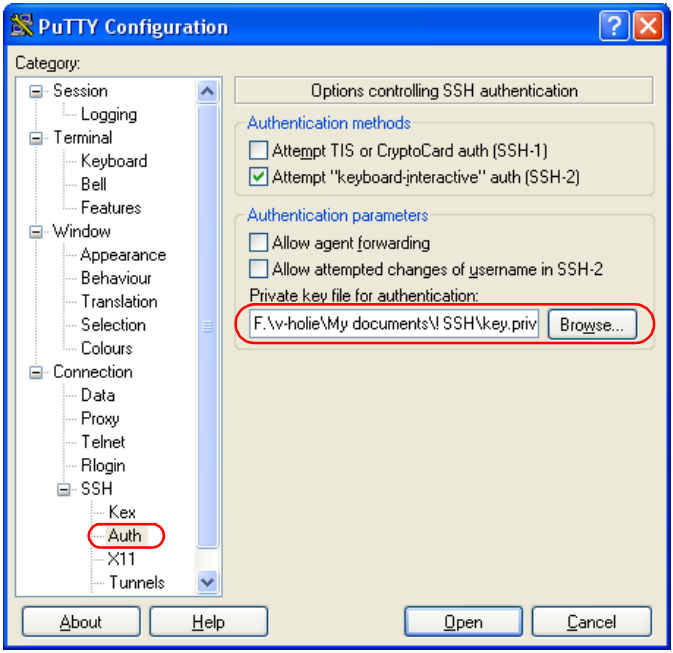


Bild 27: Optionen für die SSH-Authentifizierung konfigurieren

► Wählen Sie die Datei, die den privaten Schlüssel enthält, den Sie mit dem iRMC S2/S3 verwenden wollen.

Beachten Sie:
An dieser Stelle wird der private Schlüssel (siehe Seite 79) benötigt und **nicht** der öffentliche Schlüssel, den Sie auf den iRMC S2/S3 geladen haben.

Zusätzlich können Sie unter *Connection - Data* eine Benutzernamen für das Auto-Login am iRMC S2/S3 angeben:

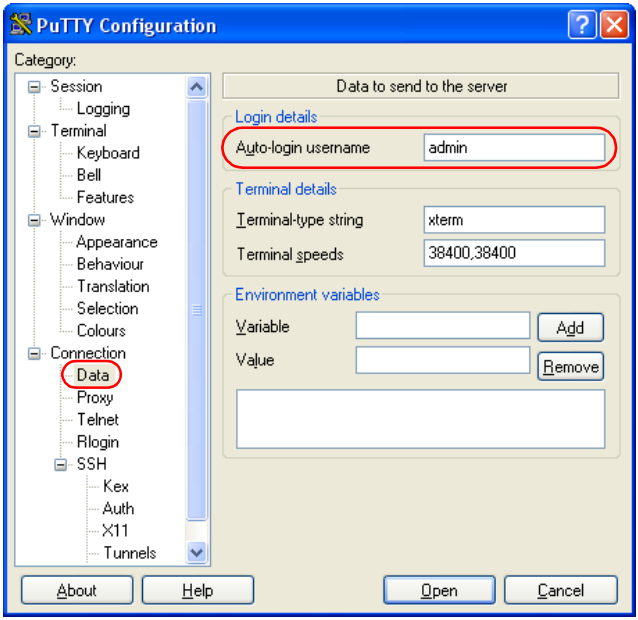


Bild 28: PuTTY: Benutzernamen für Auto-Login am iRMC S2/S3 angeben.

OpenSSH Client-Programm ssh für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren

Mithilfe des OpenSSH Client-Programms *ssh* stellen Sie eine SSHv2-gesicherte Verbindung zum iRMC S2/S3 her. Dabei können Sie sich wahlweise unter Ihrer aktuellen lokalen Benutzerkennung oder einer anderen Benutzerkennung anmelden.

Voraussetzung ist, dass die betreffende Benutzerkennung als lokale Benutzerkennung am iRMC S2/S3 konfiguriert ist und der zugehörige öffentliche SSHv2-Schlüssel auf den iRMC S2/S3 geladen wurde.

ssh liest seine Konfigurationsoptionen der Reihe nach aus folgenden Quellen:

1. Kommandozeilen-Argumente, die Sie beim Aufruf von *ssh* angeben.
2. benutzerspezifische Konfigurationsdatei (*$HOME/.ssh/config*)

   Obwohl diese Datei in der Regel keine sicherheitskritischen Informationen enthält, sollte Lese-/Schreibberechtigung lediglich für den Eigentümer bestehen. Allen anderen Benutzern sollte der Zugriff verweigert werden.

3. systemweite Konfigurationsdatei (*/etc/ssh/ssh_config*)

   Diese Datei enthält Default-Werte für Konfigurationsparameter,

   – wenn keine benutzerspezifische Konfigurationsdatei existiert oder

   – wenn die entsprechenden Parameter nicht in der benutzerspezifischen Konfigurationsdateispezifiziert sind.

Für jede Option gilt der zuerst gefundene Wert.

Ausführliche Informationen zu Konfiguration und Operanden von *ssh* finden Sie auf den Man Pages von OpenSSH unter

http://www.openssh.org/manual.html

Gehen Sie wie folgt vor:

- Starten Sie *ssh*, um sich SSHv2-authentifiziert am iRMC S2/S3 anzumelden:

  ```
  ssh -l [<benutzer>] <iRMC_S2/S3>
  ```

  oder

  ```
  ssh [<benutzer>@]<iRMC_S2/S3>
  ```

  <benutzer>
  : Benutzername, unter dem Sie sich am iRMC S2/S3 anmelden wollen. Wenn Sie <benutzer> nicht angeben, verwendet *ssh* für die Anmeldung am iRMC S2/S3 den Benutzernamen, unter dem Sie an Ihrem lokalen Computer angemeldet sind.

  <iRMC_S2>
  : iRMC S2/S3-Name oder IP-Adresse des iRMC S2/S3, an dem Sie sich anmelden wollen.

Beispiel: SSHv2-authentifizierte Anmeldung am iRMC S2/S3

Für den folgenden *ssh*-Aufruf wird vorausgesetzt, dass mit *ssh-keygen* ein Paar aus privatem und öffentlichem RSA-Schlüssel analog dem "Beispiel: RSA-Schlüsselpaar mit ssh -keygen generieren" auf Seite 80 erzeugt wurde und dass der öffentliche Schlüssel *Benutzer1/.ssh/id_rsa.pub* auf für einen iRMC S2-Benutzer *user4* den iRMC S2/S3 geladen wurde (siehe Seite 82).

Sie können sich dann von Ihrem lokalen Computer unter *$HOME/Benutzer1* wie folgt am iRMC S2 „RX100_S52-iRMC“ unter der Benutzerkennung *user4* anmelden:

```
ssh user4@RX100_S52-iRMC
```

4.3.3.4 Beispiel: Öffentlicher SSHv2-Schlüssel

Im Folgenden ist derselbe öffentliche SSHv2-Schlüssel sowohl im Format gemäß RFC4716 als auch im OpenSSH-Format abgedruckt.

Öffentlicher SSHv2 Schlüssel im Format gemäß RFC4716

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

Öffentlicher SSHv2 Schlüssel im OpenSSH-Format

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+F
pGJ2iw== rsa-key-20090401
```

5 Grafische Konsolen-Umleitung (AVR)

Die Nutzung der Funktion „Grafische Konsolen Umleitung (Advanced Video Redirection“) setzt einen gültigen Lizenzschlüssel (License Key) voraus.

Mit der Grafische Konsolen-Umleitung (Advanced Video Redirection, AVR) können Sie von Ihrem Remote-Arbeitsplatz aus Tastatur und Maus des verwalteten Servers kontrollieren und sich die aktuellen grafischen Ausgaben sowie die Text-Ausgaben des verwalteten Servers anzeigen lassen.

Über das Java-Applet der AVR können Sie die Funktion „Remote Storage“ nutzen (siehe Kapitel "Remote Storage" auf Seite 117).

Das vorliegende Kapitel informiert über folgende Themen:

– Einstellungen für die AVR prüfen
– AVR verwenden
– Menüs des AVR-Fensters

5.1 Voraussetzungen: Die Einstellungen für die AVR überprüfen

Bevor Sie AVR nutzen, prüfen Sie folgende wichtige Einstellungen:

Einstellungen für den Grafikmodus am verwalteten Server

AVR unterstützt die folgenden Grafikmodi:

Auflösung	Wiederholungs-raten [in Hz]	maximale Farbtiefe [bit]
640 x 480 (VGA)	60; 75; 85	32
800 x 600 (SVGA)	56; 60; 72; 75; 85	32
1024 x 768 (XGA)	60; 70; 75; 85	32
1152 x 864	60; 70; 75	32
1280 x 1024 (UXGA)	60; 70; 75; 85	16
1280 x 1024 (UXGA)	60	24
1600 x 1200 (UXGA)	60; 65	16
1600 x 1200 (UXGA)	60; 65	16
1680 x 1050[1]	60	16
1920 x 1080[1]	60	16
1920 x 1200[1]	60	16

Tabelle 3: Unterstützte Einstellungen für die Bildanzeige

[1] Nur iRMC S3.

Wenn am Server ein Grafikmodus mit hoher Auflösung eingestellt ist (in Tabelle grau hinterlegt), wird dies an der iRMC S2/S3-Web-Schnittstelle angezeigt.

Es werden ausschließlich VESA-konforme Grafikmodi unterstützt.

Unterstützter Text-Modus

Der iRMC S2/S3 unterstützt die folgenden gebräuchlichen Text-Modi:

– 40 x 25
– 80 x 25
– 80 x 43
– 80 x 50

Für Informationen zu den Einstellungen für die Bildanzeige siehe die Hilfe zum Betriebssystem.

Tastatur-Einstellungen

Die Einstellungen für die Tastatur müssen identisch sein:

– am Remote-Arbeitsplatz
– am verwalteten Server
– am iRMC S2/S3

5.2 AVR verwenden

- Um die AVR zu starten, klicken Sie in der Seite *Grafische Konsolen Umleitung (AVR)* der iRMC S2/S3-Web-Oberfläche auf die Schaltfläche *Video Umleitung Starten* oder *Video Umleitung starten (Java Web Start)* (siehe Seite 312).

  Es wird dann das Fenster *iRMC S2/S3 Video Umleitung* (AVR-Fenster) geöffnet, das die Bildschirmausgabe am verwalteten Server darstellt.

  Zusätzlich enthält das AVR-Fenster folgende Elemente:

  – Menüleiste: Über die Menüs *Präferenzen* und *Extras* können sie die Einstellungen der AVR konfigurieren und die AVR steuern (siehe Seite 108). Über *Remote Storage* rufen Sie Remote Storage auf (siehe Seite 112).
  Über *Sprachen* (siehe Seite 114) legen Sie fest, in welcher Landessprache (Deutsch/Englisch) die Menüs und Dialoge des AVR-Fensters angezeigt werden.

  – Integrierte Sondertasten (siehe Seite 98).

  – Die Anzeige *Lokaler Bildschirm <Status>* informiert, ob der lokale Bildschirm des verwalteten Servers eingeschaltet ist (siehe Abschnitt "„Lokaler Bildschirm Aus“-Funktionalität" auf Seite 97).

Bild 29: Fenster iRMC S2/S3 Video Umleitung (AVR-Fenster)

5.2.1 Geringe Bandbreite verwenden

Für den Fall, dass nur eine eingeschränkte Datentransfer-Rate verfügbar ist, können Sie für die Dauer Ihrer aktuellen AVR-Sitzung eine geringere Bandbreite (Bits pro Pixel, BPP) hinsichtlich der Farbtiefe konfigurieren (siehe Seite 116).

5.2.2 Parallele AVR-Sitzungen

AVR kann von zwei Benutzer-Sitzungen gleichzeitig verwendet werden. Dabei hat einer der Benutzer die volle Kontrolle über den Server („Volle Kontrolle“-Modus), während der andere Benutzer die Bedienung des Servers via Tastatur- und Mauseingaben nur passiv verfolgen kann („Nur Lesen“-Modus).

Nach dem Start der AVR befinden Sie sich zunächst im „Nur Lesen“-Modus. Sie werden in jedem Fall gefragt, ob Sie in den „Volle Kontrolle“-Modus wechseln wollen. Falls Sie sich für den „Volle Kontrolle“-Modus entscheiden und es ist bereits eine andere AVR-Sitzung im „Volle Kontrolle“-Modus aktiv, wird die bereits bestehende Sitzung in den „Nur Lesen“-Modus versetzt.

5.2.3 „Lokaler Bildschirm Aus“-Funktionalität

Die *Lokaler Bildschirm Aus*-Funktionalität des iRMC S2/S3 bietet Ihnen die Möglichkeit, den lokalen Bildschirm des verwalteten Servers für die Dauer Ihrer AVR-Sitzung auszuschalten. Auf diese Weise stellen Sie sicher, dass am lokalen Bildschirm des Servers Ihre via AVR durchgeführten Eingaben und Aktionen nicht sichtbar sind. Am Server wird „Lokaler Bildschirm aus“ durch Blinken der Identifizierungs-LED signalisiert.

Die „Lokaler Bildschirm aus“-Funktionalität konfigurieren Sie über die Seite *Grafische Konsolen Umleitung (AVR)* der iRMC S2/S3-Web-Oberfläche (siehe Seite 312). Nach entsprechender Konfiguration können Sie den lokalen Bildschirm des Servers vom Remote-Arbeitsplatz aus wie folgt ein- und ausschalten:

– im „Volle Kontrolle“-Modus einer AVR-Sitzung über das Menü *Extras*

– mit Administrator- oder OEM-Berechtigung direkt auf der Seite *Grafische Konsolen Umleitung (AVR)*

Zusätzlich können Sie konfigurieren, dass sich der lokale Bildschirm beim Start einer neuen AVR-Sitzung immer automatisch ausschaltet.

Der aktuelle Status des lokalen Bildschirms wird im AVR-Fenster oben rechts neben den integrierten Sondertasten als blauer Schriftzug angezeigt:

Lokaler Bildschirm ist immer ein
: Der lokale Bildschirm ist immer eingeschaltet und kann nicht ausgeschaltet werden, da die Option *Lokaler Bildschirm Aus* (siehe Seite 317) deaktiviert ist.

Lokaler Bildschirm ist eingeschaltet
: Der lokale Bildschirm ist eingeschaltet, kann aber ausgeschaltet werden.

Lokal Bildschirm ist ausgeschaltet
: Der lokale Bildschirm ist ausgeschaltet, kann aber eingeschaltet werden.

Lokaler Bildschirm ist immer aus
: Der lokale Bildschirm ist immer ausgeschaltet und kann nicht eingeschaltet werden, da am verwalteten Server ein Grafikmodus mit hoher Auflösung eingestellt ist (siehe Tabelle 3 auf Seite 92).

5.2.4 Umleitung der Tastatur

Die Tastatur-Umleitung funktioniert nur, wenn das AVR-Fenster den Eingabe-Fokus hat:

- Falls die Tastatur-Umleitung nicht zu funktionieren scheint, klicken Sie einfach auf das AVR-Fenster.
- Falls die Tastatur nicht reagiert, überprüfen Sie, ob sich das AVR-Fenster im „Nur Lesen“-Modus befindet. Wie Sie in den „Volle Kontrolle“-Modus umschalten, ist auf Seite 110 beschrieben.

Besondere Tastenkombinationen

AVR überträgt alle normalen Tastenkombinationen an den Server. Sondertasten, wie z.B. Windows-Tasten, werden nicht übertragen. Einige spezielle Tastenkombinationen, wie z.B. ALT + F4, können nicht übertragen werden, da sie vom Betriebssystem des Client abgefangen werden. In diesen Fällen behelfen Sie sich mit den integrierten Sondertasten oder der virtuellen Tastatur.

Integrierte Sondertasten

Unterhalb der Menüleiste finden Sie im AVR-Fenster die Leiste mit den Sondertasten. Diese Tasten sind als „Sticky Key“ implementiert, d.h. sie bleiben nach Anklicken „gedrückt“ und werden erst durch erneutes Anklicken in die Grundstellung zurückgesetzt.

Mithilfe der integrierten Sondertasten können Sie z.B. Windows-Tasten oder spezielle Tastenkombinationen nutzen, die bei Eingabe über Ihre Tastatur nicht via AVR übertragen werden können.

Bild 30: AVR-Fenster - Integrierte Sondertasten

Maus Sync
: Durch Drücken dieser Taste synchronisieren Sie die Mauszeiger (siehe auch Abschnitt "Mauszeiger synchronisieren" auf Seite 100).

Strg
: Linke Kontrolltaste (entspricht der Taste Strg (Ctrl) auf Ihrer Tastatur).

Alt

Alt(ernate)-Taste (entspricht der Taste Alt auf Ihrer Tastatur).

Win

Linke und rechte Windows-Taste (entsprechen auf Ihrer Tastatur den Tasten Strg und Alt bzw. Alt Gr und Strg).

Alt Gr

Alt(ernate) Gr(aphic)-Taste (entspricht der Taste Alt Gr auf Ihrer Tastatur).

Kontext

Kontext-Menü für das markierte Objekt (entspricht der Tastenkombination Shift + F10 auf Ihrer Tastatur).

Lock

Feststelltaste (entspricht der Taste Caps Lock auf Ihrer Tastatur).

Strg-Alt-Entf

Entspricht der Tastenkombination Strg + Alt + Entf auf Ihrer Tastatur.

Virtuelle Tastatur

Die „virtuelle Tastatur“ (siehe Bild 31) bietet Ihnen eine bedienbare Abbildung der Tastatur. Bei Verwendung der virtuellen Tastatur stehen Ihnen alle Tastenkombination zur Verfügung. Somit können Sie die virtuelle Tastatur als vollwertige Alternative für eine reale Tastatur bedienen.

Die virtuelle Tastatur aktivieren Sie im AVR-Fenster über das Menü *Extras* (siehe Seite 109).

Virtuelle Tastatur
Tastatur
ESC F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12
PSC Slk brk
Lock
` 1 2 3 4 5 6 7 8 9 0 - = BackSp
INS HM PUP
NLk / * -
Tab q w e r t y u i o p [ ] \
DEL END PDN
7 8 9 +
Caps a s d f g h j k l ; ' Enter
4 5 6
Shift z x c v b n m , . / Shift
1 2 3 ENT
Ctrl Alt Alt Ctrl
0 .

Bild 31: virtuelle Tastatur (Tastatur-Layout: Deutsch (DE)

Sichere Tastatur (Secure Keyboard)

Wenn Sie über eine HTTPS-Verbindung mit der iRMC S2/S3-Web-Oberfläche verbunden sind, werden die Tastatureingaben SSL-gesichert übertragen.

5.2.5 Umleitung der Maus

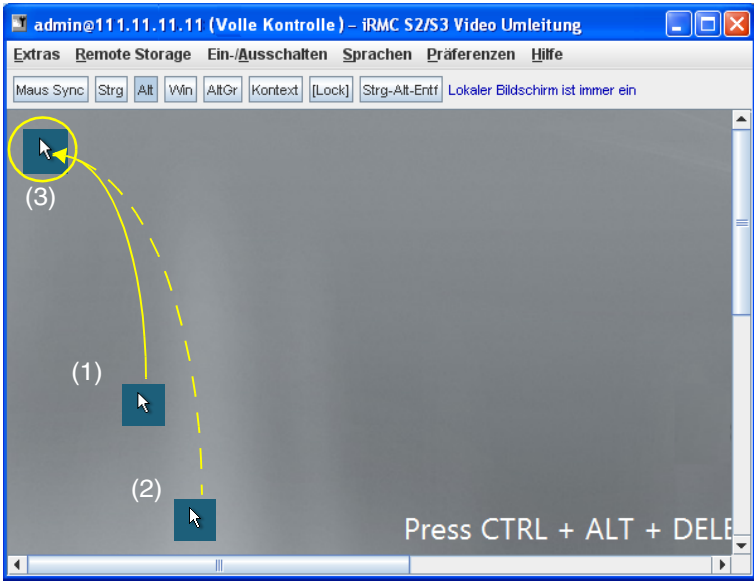
Der Mauszeiger des verwalteten Servers wird synchron mit der Maus am Remote-Arbeitsplatz bewegt. Die Einstellungen für die Umleitung der Maus konfigurieren Sie im AVR-Fenster über das Menü *Präferenzen* (siehe Seite 115).

5.2.5.1 Mauszeiger synchronisieren

Möglicherweise ist nach dem Öffnen des AVR-Fensters der Mauszeiger am Remote-Arbeitsplatz (lokaler Mauszeiger) noch nicht mit dem Mauszeiger am verwalteten Server synchronisiert.

Um beide Mauszeiger zu synchronisieren, verfahren Sie wahlweise nach einer der beiden folgenden Alternativen (siehe Bild 32 auf Seite 101):

- Drücken Sie in der Menü-Leiste des AVR-Fensters die Taste Maus Sync.
- Ziehen Sie den lokalen Mauszeiger in die linke obere Ecke des AVR-Fensters. Der Mauszeiger des verwalteten Servers folgt automatisch. Sobald sich beide Mauszeiger vollständig überlappen, sind die Zeiger synchronisiert.


admin@111.11.11.11 (Volle Kontrolle) – iRMC S2/S3 Video Umleitung
Extras Remote Storage Ein-/Ausschalten Sprachen Präferenzen Hilfe
Maus Sync Strg Alt Win AltGr Kontext [Lock] Strg-Alt-Entf Lokaler Bildschirm ist immer ein
(3)
(1)
(2)
Press CTRL + ALT + DELE

Maus Sync -Taste drücken

oder

(1) Lokalen Mauszeiger in die linke obere Ecke ziehen.

(2) Mauszeiger des Servers folgt automatisch.

(3) Die Mauszeiger sind synchronisiert, wenn sie sich vollständig überlappen und im AVR-Fenster als **ein** Mauszeiger dargestellt werden.

Bild 32: Lokalen Mauszeiger und Mauszeiger des verwalteten Servers synchronisieren.

Die einwandfreie Synchronisation der Mauszeiger erfordert bestimmte Einstellungen am verwalteten Server. Wenn der verwaltete Server mithilfe des ServerView Installation Managers installiert wurde, sind die erforderlichen Einstellungen durch die Matrox VGA Treiber-Installation bereits automatisch vorkonfiguriert worden.

Wenn die Synchronisation der Mauszeiger nicht optimal funktioniert, z.B. weil die vorkonfigurierten Einstellungen verändert wurden, oder weil der verwaltete Server nicht via Installation Manager installiert wurde, können Sie mit den im Folgenden beschriebenen Einstellungen die einwandfreie Synchronisation der Mauszeiger wiederherstellen. Diese Einstellungen sind für den verwalteten Server vorzunehmen.

Die Einstellungen für die Mauszeiger-Synchronisation werden nur für das Betriebssystem unterstützt, das auf dem verwalteten Server läuft.

Falls die Software zur Steuerung des Mauszeigers aktiv ist, kann der Mauszeiger nicht immer synchronisiert werden.

5.2.5.2 Verwalteter Windows Server: Einstellungen für Mauszeiger-Synchronisation anpassen

Für einen Windows Server können Sie die Einstellungen für die Mauszeiger-Synchronisation wahlweise via Batch-Programm oder über das Windows Startmenü und Kontext-Menü modifizieren.

Folgende Einstellungen müssen Sie anpassen:

- Geschwindigkeit des Mauszeigers
- Hardwarebeschleunigung

Wenn Sie die Einstellungen via Batch-Programm anpassen, wird zusätzlich zur Anpassung von Mauszeiger-Geschwindigkeit und Hardwarebeschleunigung der Matrox Grafik-Treiber installiert.

Alle Einstellungen für den verwalteten Server können Sie wahlweise direkt am verwalteten Server oder via AVR vom Remote-Arbeitsplatz aus vornehmen.

Einstellungen am verwalteten Server via Batch-Programm anpassen

Gehen Sie wie folgt vor:

- ► Öffnen Sie die Windows-Eingabeaufforderung.
- ► Wechseln Sie in das Verzeichnis, in dem das Batch-Programm *install_kronos2_vga.bat* der jeweiligen Matrox VGA Treiber-Installation (32 Bit oder 64 Bit) gespeichert ist.

  Standardmäßig finden Sie die Programme *install_kronos2_vga.bat* unter:

  C:\Programme\Fujitsu\ServerView Suite\Installation Manager\Content\V10.09.12.00\DRV\VIDEO\MATROX\iRMC\W2K

  sowie auf Ihrer ServerView Suite DVD 1.
- ► Geben Sie *setup.bat* ein und starten Sie das Batch-Programm.
- ► Starten Sie nach Ausführung des Batch-Programms den verwalteten Server neu.

Einstellungen am verwalteten Server über Windows Start- und Kontext-Menü anpassen

Zur Anpassung des Mauszeigers gehen Sie wie folgt vor:

► Wählen Sie

Start - Einstellungen - Systemsteuerung - Drucker und andere Hardware - Maus - Registerkarte - *Zeigeroptionen*.

Das folgende Fenster wird angezeigt:

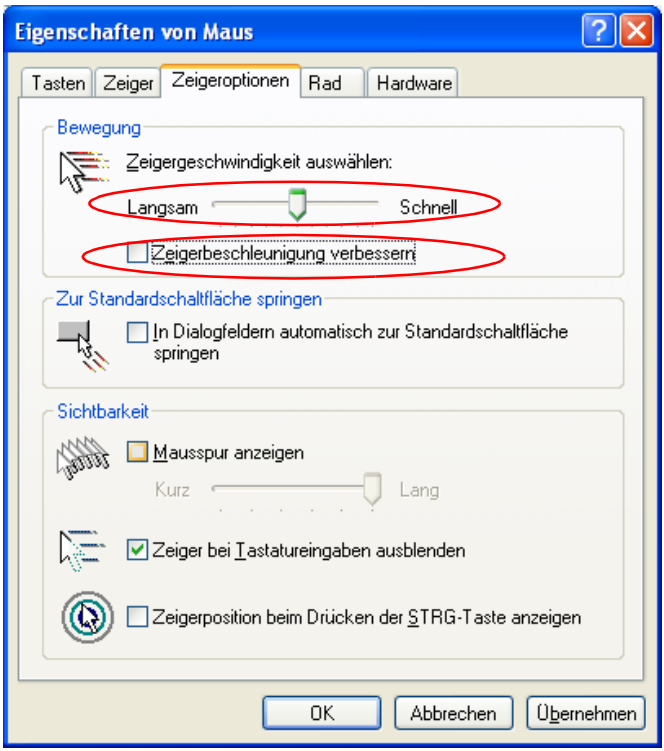


Bild 33: Eigenschaften von Maus - Zeigeroptionen

► Setzen Sie die *Zeigergeschwindigkeit* auf einen mittleren Wert.

► Deaktivieren Sie die Option *Zeigerbeschleunigung verbessern*.

► Klicken Sie auf die Schaltfläche OK, um die Einstellungen zu sichern.

Zur Anpassung der Hardwarebeschleunigung gehen Sie wie folgt vor:

- Klicken Sie mit der rechten Maustaste auf den Hintergrund.
- Wählen Sie im Kontextmenü:

  Eigenschaften - Registerkarte *Einstellungen* - Schaltfläche *Erweitert* - Registerkarte *Problembehandlung*.

  Das folgende Fenster wird angezeigt:

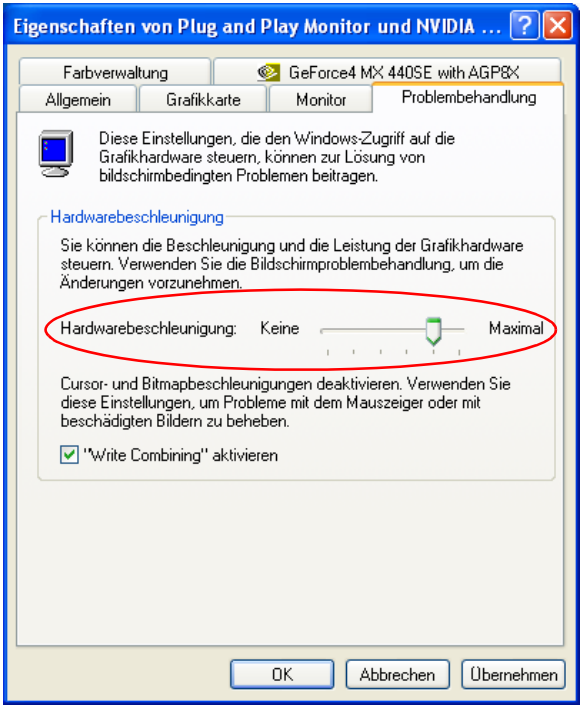

Eigenschaften von Plug and Play Monitor und NVIDIA ...
Farbverwaltung
GeForce4 MX 440SE with AGP8X
Allgemein
Grafikkarte
Monitor
Problembehandlung
Diese Einstellungen, die den Windows-Zugriff auf die Grafikhardware steuern, können zur Lösung von bildschirmbedingten Problemen beitragen.
Hardwarebeschleunigung
Sie können die Beschleunigung und die Leistung der Grafikhardware steuern. Verwenden Sie die Bildschirmproblembehandlung, um die Änderungen vorzunehmen.
Hardwarebeschleunigung:
Keine
Maximal
Cursor- und Bitmapbeschleunigungen deaktivieren. Verwenden Sie diese Einstellungen, um Probleme mit dem Mauszeiger oder mit beschädigten Bildern zu beheben.
"Write Combining" aktivieren
OK
Abbrechen
Übernehmen

Bild 34: Eigenschaften - ... - Problembehandlung: Hardwarebeschleunigung

- Setzen Sie die *Hardwarebeschleunigung* auf einen Wert wie in Bild 34.
- Klicken Sie auf die Schaltfläche OK, um die Einstellungen zu sichern.

5.2.5.3 Verwalteter Linux Server: Einstellungen für Mauszeiger-Synchronisation anpassen

Voraussetzung: Der verwaltete Server läuft unter einem der folgenden Linux-Betriebssysteme:

– Red Hat 4.x
– Red Hat 5.x
– Suse 9.x
– Suse 10.x
– Suse 11.x

Für Suse Linux und Redhat Linux gibt es verschieden grafische Benutzeroberflächen (GUI). Die wichtigsten GUIs sind:

– Gnome
– KDE

Die Einstellungen für die Mauszeiger-Synchronisation können Sie auf dem verwalteten Server wahlweise per Kommando oder Menü-geführt anpassen.

Folgende Einstellungen müssen Sie anpassen:

– *Mouse motion acceleration* = 1
– *Mouse motion threshold* =1

Alle Einstellungen für den verwalteten Server können Sie wahlweise direkt am verwalteten Server oder via AVR vom Remote-Arbeitsplatz aus vornehmen.

Temporäre Einstellungen am verwalteten Server via Kommando anpassen

Mit dem Kommando *xset* setzen Sie die Einstellungen für *Pointer acceleration* und *Pointer threshold* (empfohlene Werte: jeweils 1) für die Dauer der aktuellen Session.

Kommando-Syntax:

`xset m(ouse)][`*acceleration*`][`*threshold*`]`

Gehen Sie wie folgt vor:

► Rufen Sie ein Kommandozeilen-Tool auf.

► Führen Sie das Kommando *xset* mit folgenden Argumenten aus:

```
xset m 1 1
```

Permanente Einstellungen am verwalteten Server via Konfigurationsdatei anpassen (KDE)

Für **KDE** nehmen Sie permanente Einstellungen wie folgt vor:

- Ändern Sie die Einstellungen der Text-Datei */root/.kde/share/config/kcminputrc* wie folgt:

```
[Mouse]
Acceleration=1
Threshold=1
```

Ein erneutes Setzen der Werte nach dem Neustart des Servers ist nicht erforderlich.

Permanente Einstellungen am verwalteten Server Menü-geführt anpassen

Ein erneutes Setzen der Werte nach dem Neustart des Servers ist nicht erforderlich.

Für **KDE** nehmen Sie permanente Einstellungen wie folgt vor:

Das im Folgenden beschriebene Verfahren für KDE gilt nur für Suse Linux.

- Wählen Sie

  N - Control Center - Peripheral - Mouse - Registerkarte *Advance*

  Das Fenster *Mouse - Control Center* wird angezeigt:

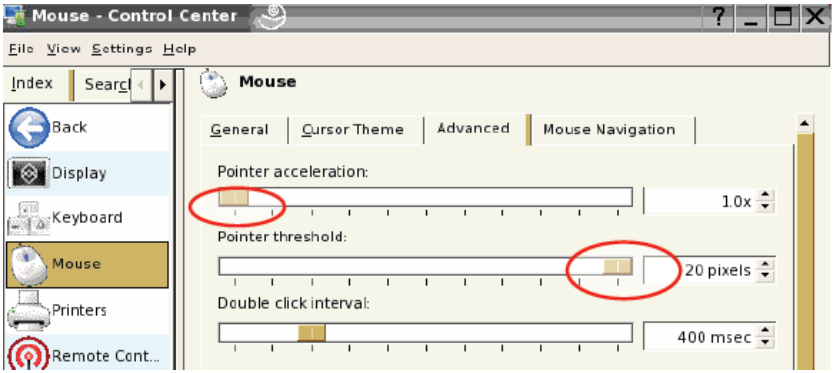


Bild 35: Fenster Mouse Control Center Window

- ► Setzen Sie im Fenster *Mouse Control Center Window* folgende Werte:
  - – *Pointer acceleration:* 1.0x (Minimalwert)
  - – *Pointer threshold:* 20 Pixel (Maximalwert)
- ► Sichern Sie die Einstellungen.
- ► Starten Sie den verwalteten Server neu.

  Ein erneutes Setzen der Werte nach dem Neustart des Servers ist nicht erforderlich.

Für **Gnome** nehmen Sie permanente Einstellungen wie folgt vor:

- ► Rufen Sie in der Shell den Editor *gconf-editor* auf.
- ► Wählen Sie: *desktop - gnome - peripherals - mouse*
- ► Ändern Sie folgende Attributwerte:

```
motion_acceleration 1
motion_threshold 1
```

5.3 Menüs des AVR-Fensters

Die Menü-Leiste des AVR-Fensters enthält folgende Menüs:

– Über das Menü *Extras* steuern Sie die AVR-Sitzung. Außerdem können Sie eine virtuelle Tastatur bereitstellen.

– Über das Menü *Remote Storage* können Sie Remote Storage Verbindungen herstellen und trennen.

– Über das Menü *Ein-/Ausschalten* können Sie den Server einschalten, ausschalten oder neu starten.

– Über das Menü *Sprachen* wählen Sie die Landessprache (Deutsch/Englisch), in der die AVR-Menüs und -Dialoge angezeigt werden.

– Über das Menü *Präferenzen* konfigurieren Sie die Einstellungen für Maus, Tastatur und Logging.

5.3.1 Menü Extras

Im Menü *Extras* können Sie zwischen folgenden Funktionen wählen:

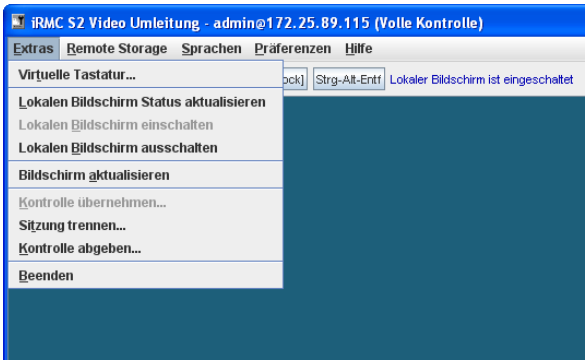


Bild 36: AVR-Fenster - Menü Extras

Virtuelle Tastatur ...

Das Fenster *Vituelle Tastatur* öffnet sich (siehe Bild 31 auf Seite 99).

Lokalen Bildschirm Status aktualisieren

Lokalen Bildschirm Status-Anzeige aktualisieren.

Lokalen Bildschirm einschalten

Lokalen Bildschirm des verwalteten Servers einschalten.

Auch wenn der lokale Bildschirm ausgeschaltet ist, ist die Funktion in folgenden Fällen deaktiviert:

- Sie befinden sich im „Nur Lesen“-Modus.
- Am verwalteten Server ist ein Grafikmodus mit hohe Auflösung eingestellt (siehe Tabelle 3 auf Seite 92).
  Lokaler Bildschirm <status>-Anzeige:
  Lokaler Bildschirm ist immer aus

Lokalen Bildschirm ausschalten

Lokalen Bildschirm des verwalteten Servers ausschalten.

Auch wenn der lokale Bildschirm eingeschaltet ist, ist die Funktion in folgenden Fällen deaktiviert:

- Sie befinden sich im „Nur Lesen“-Modus.
- Beim Start der AVR war unter *Lokaler Bildschirm* die Option *Lokaler Bildschirm Aus* nicht aktiviert (siehe Seite 316).
  Lokaler Bildschirm <status>-Anzeige:
  Lokaler Bildschirm immer ein

Bildschirm aktualisieren

AVR-Fenster aktualisieren.

Kontrolle übernehmen...

In den „Volle Kontrolle“-Modus wechseln. (Falls Sie sich bereits im „Volle Kontrolle“-Modus befinden, ist diese Funktion deaktiviert.)

Eine bereits existierende Sitzung im „Volle Kontrolle“-Modus wird durch den folgenden Dialog benachrichtigt Wenn eine bereits existierende Sitzung Ihren Versuch, in den „Volle Kontrolle“-Modus zu wechseln, zurückweist, verbleiben Sie in „Nur Lesen“-Modus.

Sitzung trennen...

Eine fremde AVR-Sitzung beenden.

Mit *Sitzung trennen...* können Sie nur fremde AVR-Sitzungen beenden. Um Ihre eigene Sitzung zu beenden, wählen Sie *Beenden*.

Es wird die Liste der aktuellen AVR-Sitzungen angezeigt:

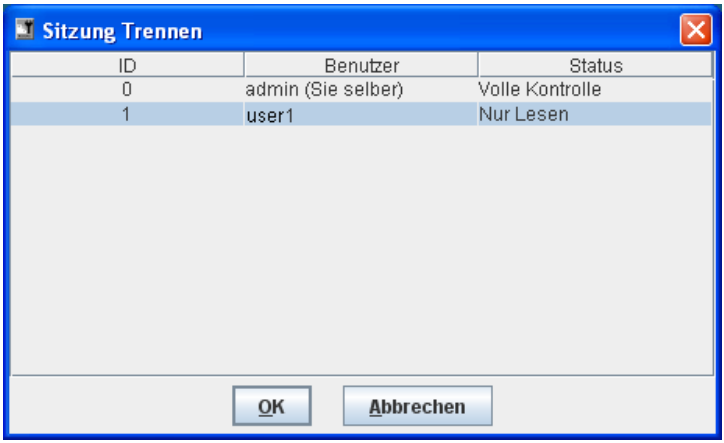


Bild 37: Menü Extras - Sitzung trennen

- ► Markieren Sie die AVR-Sitzung, die Sie beenden wollen.
- ► Bestätigen Sie mit *OK*, wenn Sie die ausgewählte AVR-Sitzung beenden wollen.
- ► Widerrufen Sie mit *Abbrechen*, wenn Sie die ausgewählte AVR-Sitzung nicht beenden wollen.

Kontrolle abgeben...

In den „Nur Lesen“-Modus wechseln. (Falls Sie sich bereits im „Nur Lesen“-Modus befinden, ist diese Funktion deaktiviert.)

Beenden

Die eigene AVR-Sitzung beenden.

5.3.2 Menü Remote Storage

Unter *Remote Storage* rufen Sie die Remote Storage-Funktionalität auf:

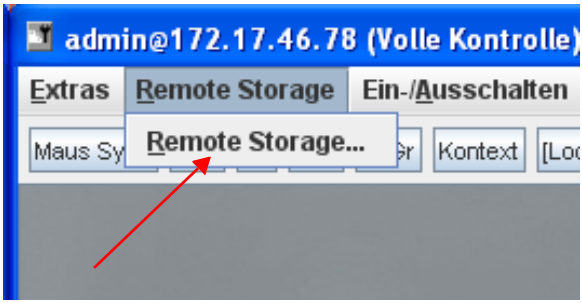


Bild 38: AVR-Fenster - Menü Remote Storage

Remote Storage...

Mit Doppelklick auf *Remote Storage...* öffnen Sie das Fenster *Remote Storage Geräte* (siehe Seite 121). In diesem Fenster können Sie Medien vom Remote-Arbeitsplatz als Remote Storage verbinden oder trennen (siehe Kapitel "Remote Storage" auf Seite 117).

5.3.3 Menü Ein-/Ausschalten

Über das Menü *Ein-/Ausschalten* können Sie den Server einschalten, ausschalten oder neu starten:

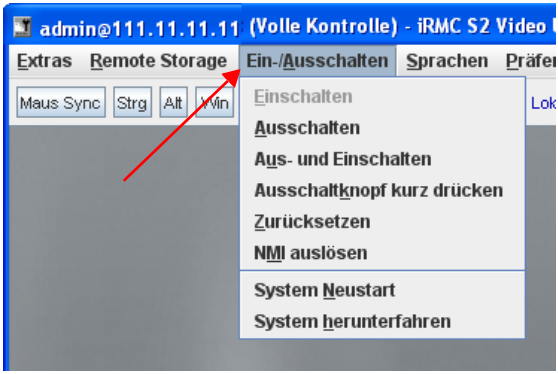


Bild 39: AVR -Fenster - Menü Ein-/Ausschalten

Einschalten

Schaltet den Server ein.

Ausschalten

Schaltet den Server aus unabhängig vom Status des Betriebssystems aus.

Aus- und Einschalten

Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein. Diese Zeit können Sie im Eingabefeld *Aus-/Einschalt Verzögerung* der Gruppe *ASR&R Einstellungen* (siehe Seite 240) konfigurieren.

Ausschaltknopf kurz drücken

Abhängig vom installierten Betriebssystem und der konfigurierten Aktion können Sie mit *Ausschaltknopf kurz drücken* unterschiedliche Aktionen auslösen wie Herunterfahren, Standby-Modus oder Ruhezustand auslösen.

Zurücksetzen

Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).

NMI auslösen

Löst eine nicht-maskierbare Unterbrechung (non-maskable interrupt, NMI) aus. Ein NMI ist eine Prozessorunterbrechung, die nicht von Standard-Unterbrechungsmaskierung des Systems ignoriert werden kann.

System Neustart

System „sanft“ herunterfahren und anschließend neu starten.
Diese Option ist nur verfügbar, wenn die ServerView-Agenten installiert und beim iRMC S2/S3 als „Connected“ gemeldet sind.

System herunterfahren

System „sanft“ herunterfahren und ausschalten.
Diese Option ist nur verfügbar, wenn die ServerView-Agenten installiert und beim iRMC S2/S3 als „Connected“ gemeldet sind.

5.3.4 Menü Sprachen

Unter *Sprachen* wählen Sie die Landessprache aus, in der die Menüs und Dialoge des AVR-Fensters angezeigt werden:

Bild 40: AVR-Fenster - Menü Sprachen

5.3.5 Menü Präferenzen

Über das Menü *Präferenzen* können Sie Maus-Modus, Tastatur-Layout globale Protokollierung (Logging) sowie eine niedrigere Bandbreite und einen internen TCP-Port konfigurieren:

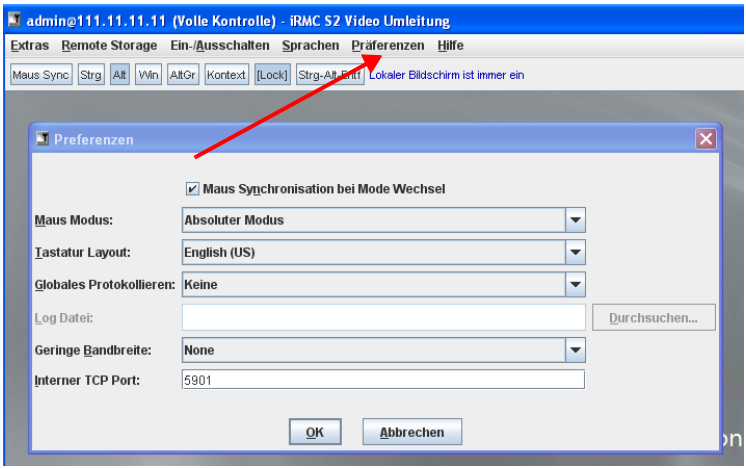

admin@111.11.11.11 (Volle Kontrolle) - iRMC S2 Video Umleitung
Extras Remote Storage Ein-/Ausschalten Sprachen Präferenzen Hilfe
Maus Sync Strg Alt Win AltGr Kontext [Lock] Strg-Alt-Entf Lokaler Bildschirm ist immer ein
Preferenzen
Maus Synchronisation bei Mode Wechsel
Maus Modus: Absoluter Modus
Tastatur Layout: English (US)
Globales Protokollieren: Keine
Log Datei:
Durchsuchen...
Geringe Bandbreite: None
Interner TCP Port: 5901
OK
Abbrechen

Bild 41: AVR-Fenster - Menü Präferenzen

Falls die Video-Umleitung Server-seitig im Modus *Num Lock On* ausgeführt wird, wechselt sie Client-seitig in den Modus *Num Lock ON*.

Maus Synchronisation bei Mode Wechsel

Voreinstellung: Aktiviert.
Legt fest, ob nach einer Änderung des Maus-Modus (siehe unten) die Mauszeiger-Synchronisation fortbestehen soll.

Maus Modus

Legt den Maus-Modus fest (*Hide Mode (Relative)*, *Absoluter Modus* oder *Relativer Modus*).

Je nach Betriebssystem des Servers sind folgende Einstellungen erforderlich:

- Windows: *Absoluter Modus*, *Hide Mode (Relative)* oder *Relativer Modus*
- Linux: *Hide Mode (Relative) oder Relativer Modus*

Voreinstellung: *Absoluter Modus*

Tastatur Layout

Legt das Tastatur-Layout für die virtuelle Tastatur fest.

Auch das Layout für die Tastatur am verwalteten Server muss entsprechend eingestellt sein, d.h. die Einstellung müssen für AVR-Client und AVR-Server identisch sein.

Globales Protokollieren

Voreinstellung: Kein globales Protokollieren.
Legt fest, ob globales Protokollieren (Logging) durchgeführt werden soll.

Globales Protokollieren muss deaktiviert sein, d.h. *Keine* muss aktiviert sein!

Log Datei

Protokolldatei für das globale Protokollieren.

Abhängig von der unter *Globales Protokollieren* gewählten Einstellung ist diese Option möglicherweise deaktiviert.

Geringe Bandbreite

Im Falle einer reduzierten Übertragungsrate können Sie hier eine verringerte Bandbreite (Einheit: bits per pixel, bpp) hinsichtlich der Farbtiefe einstellen. Die Einstellung gilt für alle AVR-Sitzungen am selben iRMC S2/S3.

None

Voreinstellung.
Keine reduzierte Bandbreite.

3 bpp

3 bpp Farbtiefe (8 Farbstufen).

8 bpp

8 bpp Farbtiefe (256 Farbstufen).

Interner TCP Port

Voreinstellung: 5901
Interner TCP Port für den integrierten Remote Storage-Client, der mit dem AVR-Client verwendet wird.

6 Remote Storage

Die Nutzung der Funktion „Remote Storage“ setzt einen gültigen Lizenzschlüssel (License Key) voraus.

Remote Storage stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich an anderer Stelle im Netz befindet. Es können bis zu zwei Medien umgeleitet werden.

Die Quelle für das virtuelle Laufwerk können Sie wie folgt bereitstellen:

– Via Remote Storage-Verbindung mithilfe des AVR Java-Applets (integrated Remote Storage-Client) als physisches Laufwerk oder Image-Datei am Remote-Arbeitsplatz (siehe Seite 119):

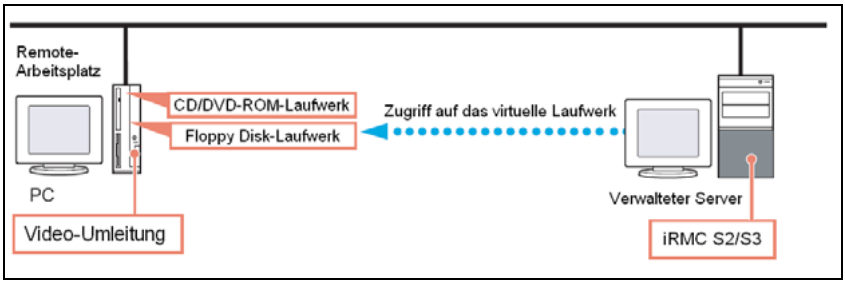


Bild 42: Remote Storage via Remote Storage-Verbindung

– Via Remote Storage Server zentral im Netz als CD/DVD ISO-Abbild (Image-Datei) (siehe Seite 133):

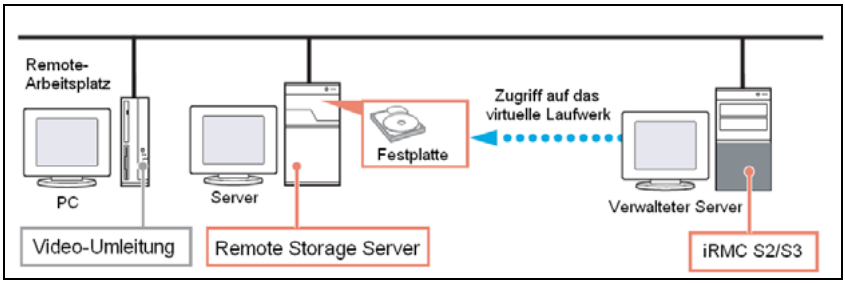


Bild 43: Remote Storage via Remote Storage Server

Parallele Remote Storage-Verbindungen:

Zur selben Zeit möglich sind entweder

– **maximal zwei** Remote Storage-Verbindungen zu virtuellen Laufwerken am Remote-Arbeitsplatz (bei Verbindungsaufbau via AVR Java-Applet)

  oder

– **eine** Remote Storage-Verbindung zu einem Remote Storage Server.

Remote Storage-Verbindungen via Applet und Remote Storage Server sind nicht gleichzeitig möglich.

Mithilfe der Seite *Remote Storage* der iRMC S2/S3-Web-Oberfläche können Sie sich über den Status der aktuellen Remote Storage-Verbindungen informieren und außerdem die Verbindung zu einem Remote Storage Server herstellen (siehe Seite 323).

6.1 Remote Storage am Remote-Arbeitsplatz bereitstellen

Wenn Sie die Quelle für ein virtuelles Laufwerk am Remote Arbeitsplatz bereitstellen, unterstützt Remote Storage folgende Gerätetypen:

– Diskette
– CD ISO Image
– DVD ISO Image
– CD, DVD

Optische Speichermedien (CD, DVD) werden automatisch angezeigt (d.h. zur Auswahl angeboten). Andere Remote Storage-Medien stellen Sie bereit, indem Sie den geeigneten Gerätetyp manuell auswählen.

Geräte, die als Remote Storage verbunden sind, werden vom iRMC S2/S3 als USB-Geräte erkannt. Die Geräte können nicht verwendet werden, falls keine USB-Verbindung verfügbar ist (z.B weil kein USB-Treiber vorhanden ist).

Mithilfe des virtuellen Laufwerks können Sie vom Remote-Arbeitsplatz aus auf Ihrem PRIMERGY Server ein Betriebssystem installieren (siehe Kapitel "Remote-Installation des Betriebssystems via iRMC S2/S3" auf Seite 385).

Der vorliegende Abschnitt informiert über folgende Themen:

– Remote Storage starten.
– Speichermedien für Remote Storage bereitstellen.
– Speichermedien als Remote Storage verbinden.
– Remote Storage-Verbindungen trennen
– Für Remote Storage bereitgestellte Speichermedien entfernen.

6.1.1 Remote Storage starten

Remote Storage starten Sie über das AVR Java Applet (siehe Abschnitt "Grafische Konsolen Umleitung (AVR) - Grafische Konsolen-Umleitung (AVR) starten" auf Seite 312):

- Starten Sie die iRMC S2/S3-Web-Oberfläche (siehe Abschnitt "An der iRMC S2/S3-Web-Oberfläche anmelden" auf Seite 142).
- Öffnen Sie die Seite *Grafische Konsolen Umleitung (AVR)* und klicken Sie auf die Schaltfläche *Video Umleitung starten,* um die grafische Konsolen-Umleitung zu starten (siehe Abschnitt "Grafische Konsolen Umleitung (AVR) - Grafische Konsolen-Umleitung (AVR) starten" auf Seite 312).

  Das AVR-Fenster wird geöffnet.
- Wählen Sie in der Menüleiste des AVR-Fensters:
  Remote Storage - RemoteStorage...

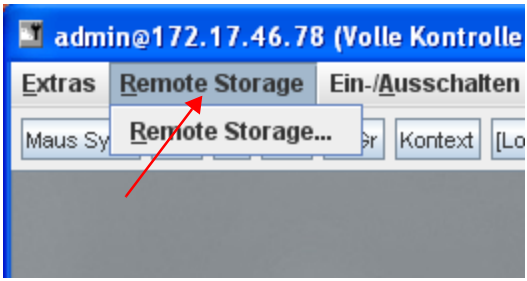


Bild 44: AVR-Fenster - Remote Storage - Remote Storage...

Der Dialog *Remote Storage Geräte* wird geöffnet, in dem die aktuell für Remote Storage bereit gestellten Speichermedien angezeigt werden.

Dialog „Remote Storage Geräte“ auf einem Windows-System

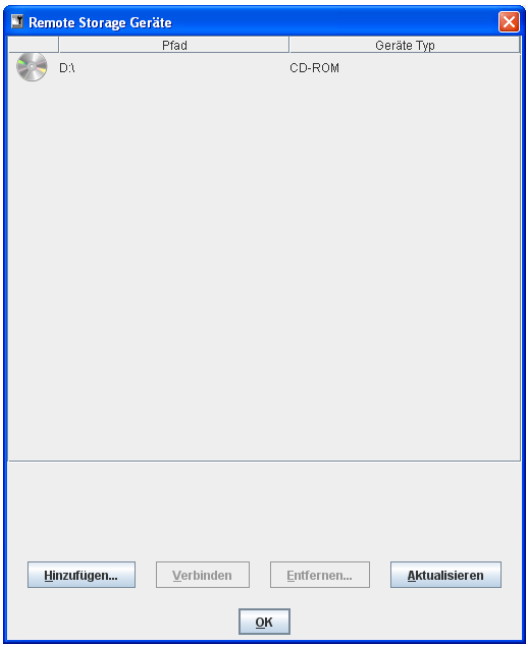


Bild 45: Dialog Remote Storage Geräte

Wenn in einem optischen Laufwerk ein Speichermedium (CD-ROM, DVD-ROM) eingelegt ist, wird das Speichermedium automatisch angezeigt.

Floppy Disk-Laufwerke sowie CD ROM- und DVD ROM-Laufwerke werden in der Liste nur dann angezeigt, wenn ein Speichermedium eingelegt ist.

Falls ein Speichermedium eingelegt ist, aber nicht angezeigt wird, ist dieses Speichermedium durch den lokalen Explorer belegt.

Dialog „Remote Storage Geräte“ auf einem Linux-System

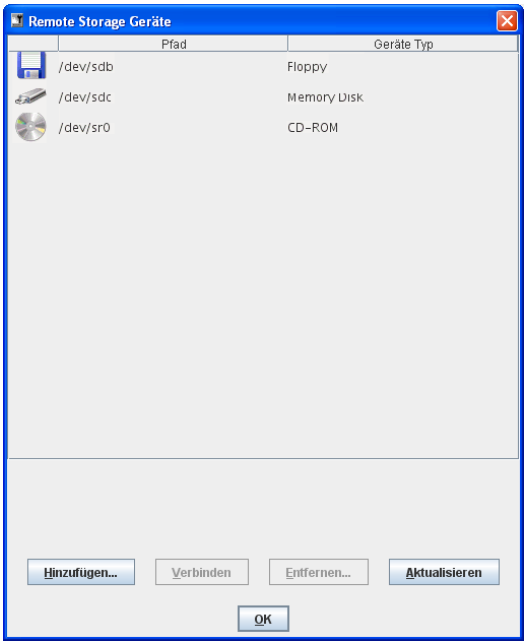


Bild 46: Dialog Remote Storage Geräte

Physische Speichermedien müssen gemountet sein, damit sie als Remote Storage verbunden werden können. Gemountete Speichermedien werden im Dialog *Remote Storage Geräte* automatisch angezeigt.

6.1.2 Speichermedien für Remote Storage bereitstellen

► Klicken Sie im Dialog *Remote Storage Geräte* auf die Schaltfläche *Hinzufügen...* .

Der Dialog *Remote Storage Gerät hinzufügen...* wird geöffnet.

Dialog „Remote Storage Geräte hinzufügen“ auf einem Windows-System

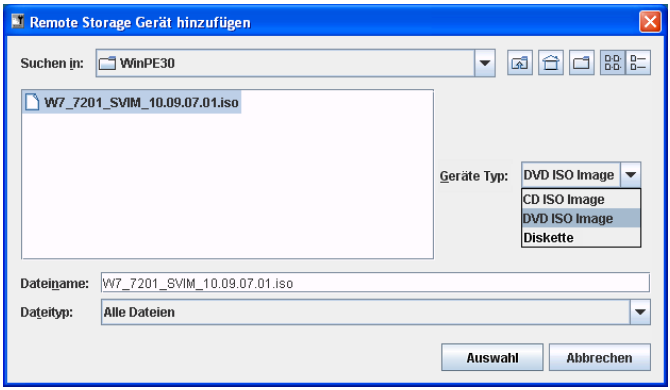


Bild 47: Dialog Remote Storage Gerät hinzufügen (Windows)

Dialog „Remote Storage Geräte hinzufügen“ auf einem Linux-System

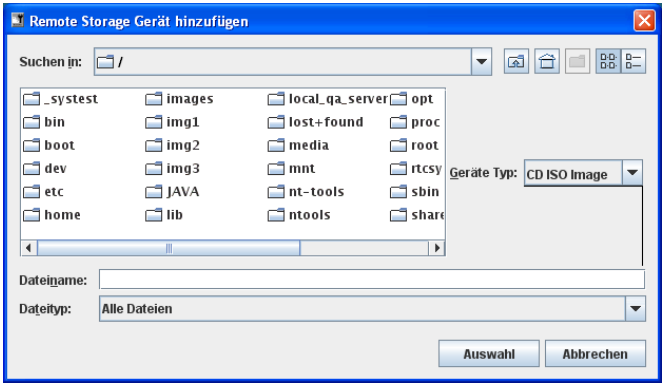


Bild 48: Dialog Remote Storage Gerät hinzufügen (Linux)

- ► Navigieren Sie im Dialog *Remote Storage Gerät hinzufügen* zum Verzeichnis des Speichermediums, das Sie von Ihrem Remote-Arbeitsplatz aus für Remote Storage bereitstellen wollen.
- ► Wählen Sie unter *Geräte Typ* den gewünschten Gerätetyp aus.

  Folgende Gerätetypen werden stehen zur Auswahl:

  – Diskette
  – CD ISO Image
  – DVD ISO Image

  Bei Linux-Systemen müssen physische Speichergeräte gemountet sein.

- ► Geben Sie unter *Dateiname* das Speichermedium an, das Sie als Remote Storage verbinden wollen:

  – Bei einem ISO-Abbild (ISO/NRG Image) geben Sie den Dateinamen an. Alternativ klicken auf den im Datei-Browser angezeigten Dateinamen.

  – Bei einem Laufwerk geben Sie den Namen des Laufwerks an, z.B.

    – „D:“ für Laufwerk D (Windows)

    – */dev/...* (Linux)

Dialog „Remote Storage Gerät hinzufügen“: Speichermedium auswählen (Windows)

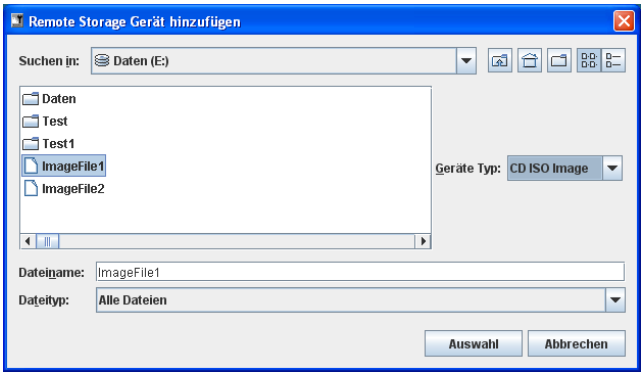


Bild 49: Dialog Remote Storage Gerät hinzufügen: Speichermedium auswählen

Dialog „Remote Storage Gerät hinzufügen“: Speichermedium auswählen (Linux)

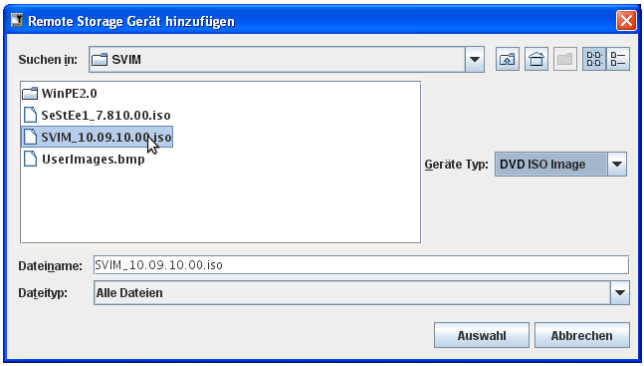


Bild 50: Dialog Remote Storage Gerät hinzufügen: Speichermedium auswählen

► Klicken Sie auf *Auswahl*, um Ihre Auswahl zu bestätigen.

Das ausgewählte Speichermedium ist für Remote Storage bereitgestellt und wird im Dialog *Remote Storage Geräte* angezeigt.

Anzeige im Dialog „Remote Storage Geräte“ (Windows)

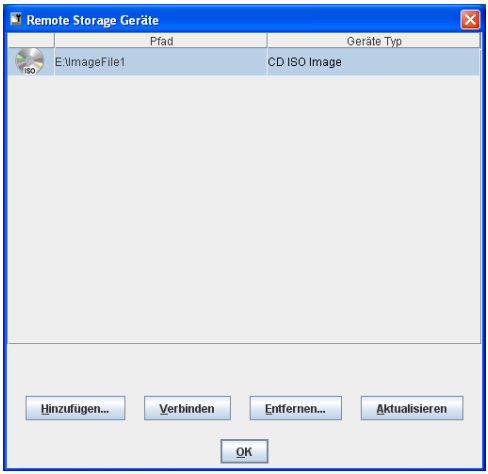


Bild 51: Dialog Remote Storage Geräte: Bereitgestelltes Speichermedium wird angezeigt.

Anzeige im Dialog „Remote Storage Geräte“ (Linux)

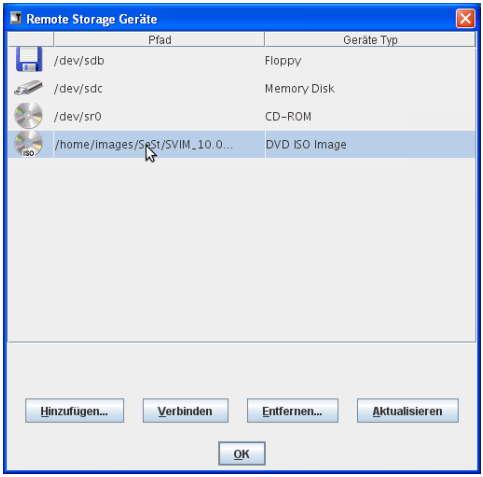


Bild 52: Dialog Remote Storage Geräte: Bereitgestelltes Speichermedium wird angezeigt.

6.1.3 Speichermedien als Remote Storage verbinden

- Markieren Sie im Dialog *Remote Storage Geräte* das Speichermedium (siehe Bild 51 bzw. Bild 52 auf Seite 126), das Sie als Remote Storage verbinden wollen.
- Klicken Sie auf *Verbinden*, um das ausgewählte Speichermedium als Remote Storage zu verbinden.

  Es wird der Dialog *Remote Storage Geräte* mit dem Hinweis auf „Sicheres entfernen“ angezeigt. Das Speichermedium ist als Remote Storage verbunden.

  Falls Sie zwei Speichermedien gleichzeitig als Remote Storage verbinden wollen, geht dem Verbindungsaufbau ein Bestätigungsdialog voraus (siehe Abschnitt "Zwei Speichermedien gleichzeitig als Remote Storage verbinden" auf Seite 129).

Dialog „Remote Storage Geräte“: Anzeige Remote Storage-Verbindung (Windows)

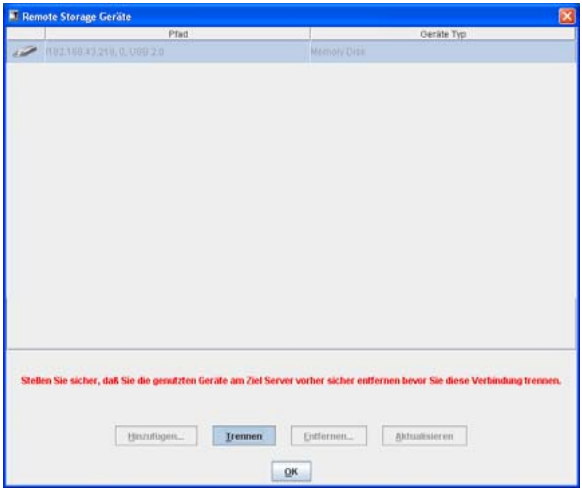


Bild 53: Dialog Remote Storage Geräte: Speichermedium als Remote Storage verbunden

Dialog „Remote Storage Geräte“: Anzeige Remote Storage-Verbindung (Linux)

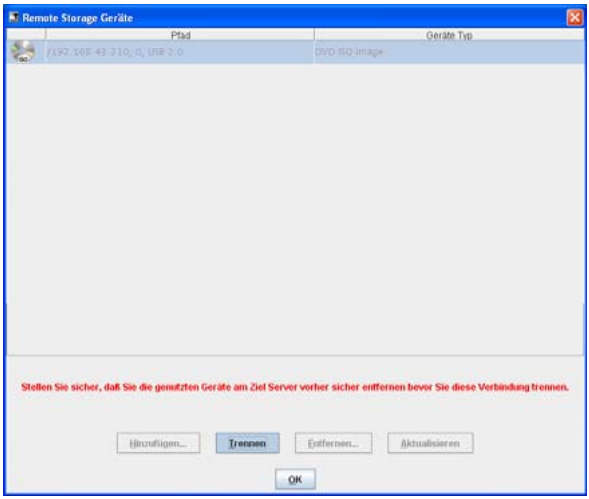


Bild 54: Dialog Remote Storage Geräte: Speichermedium als Remote Storage verbunden

Zwei Speichermedien gleichzeitig als Remote Storage verbinden

Das gleichzeitige Verbinden zweier Speichermedien als Remote Storage ist im Folgenden am Beispiel eines Windows-Systems dargestellt. Bei Linux-Systemen verfahren Sie analog.

In Bild 55 sind zwei Speichermedien als Remote Storage bereitgestellt:

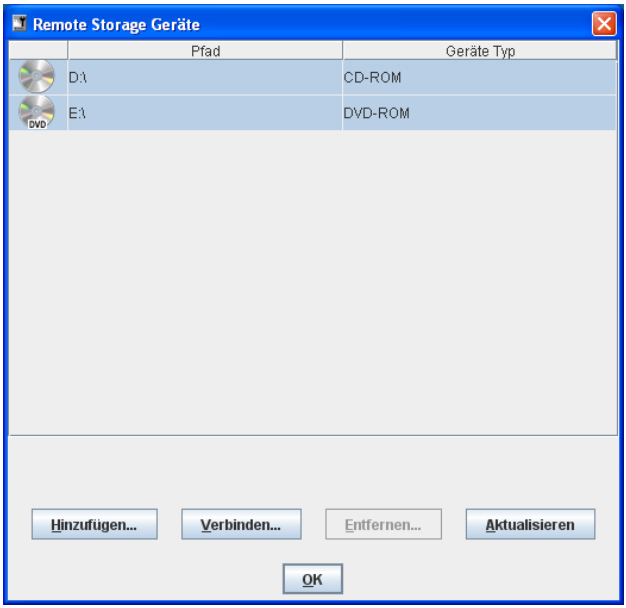


Bild 55: Dialog Remote Storage Geräte: 2 Speichermedien als Remote Storage bereitgestellt

- Markieren Sie die beiden Speichermedien und klicken Sie auf die Schaltfläche *Verbinden*, um die Speichermedien als Remote Storage zu verbinden.

  Sie erhalten dann zunächst einen Vorschlag über die Zuordnung Ihrer Speichermedien zu USB 1.1 und USB 2.0 (siehe Bild 55 auf Seite 129).

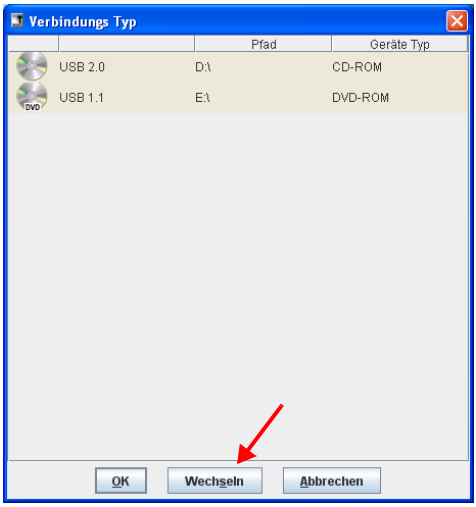


Bild 56: Dialog Verbindungs Typ: Zuordnung zu USB 1.1 und USB 2.0

► Klicken Sie auf die Schaltfläche *Wechseln*, falls Sie die Zuordnung der Speichermedien zu USB 1.1 und USB 2.0 vertauschen wollen.

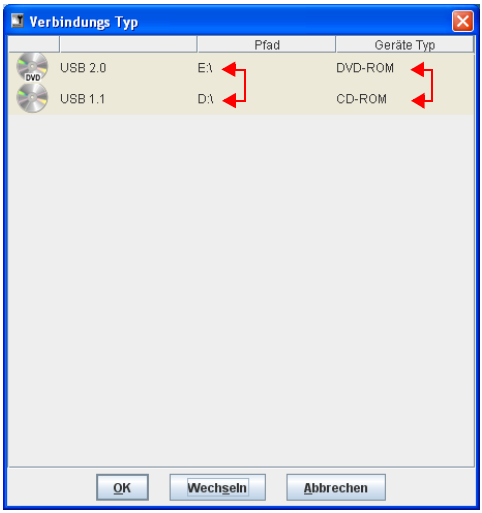


Bild 57: Dialog Verbindungs Typ: Zuordnung zu USB 1.1 und USB 2.0 geändert.

► Klicken Sie auf *OK*, um die Speichermedien als Remote Storage zu verbinden.

6.1.4 Remote Storage-Verbindungen trennen

Bei Trennung der AVR-Sitzung wird die Remote Storage-Verbindung automatisch freigegeben.

► Öffnen Sie den Dialog *Remote Storage Geräte* (siehe Abschnitt "Remote Storage starten" auf Seite 120).

Die Liste der als Remote Storage verbundenen Speichermedien wird angezeigt (Beispiel Windows).

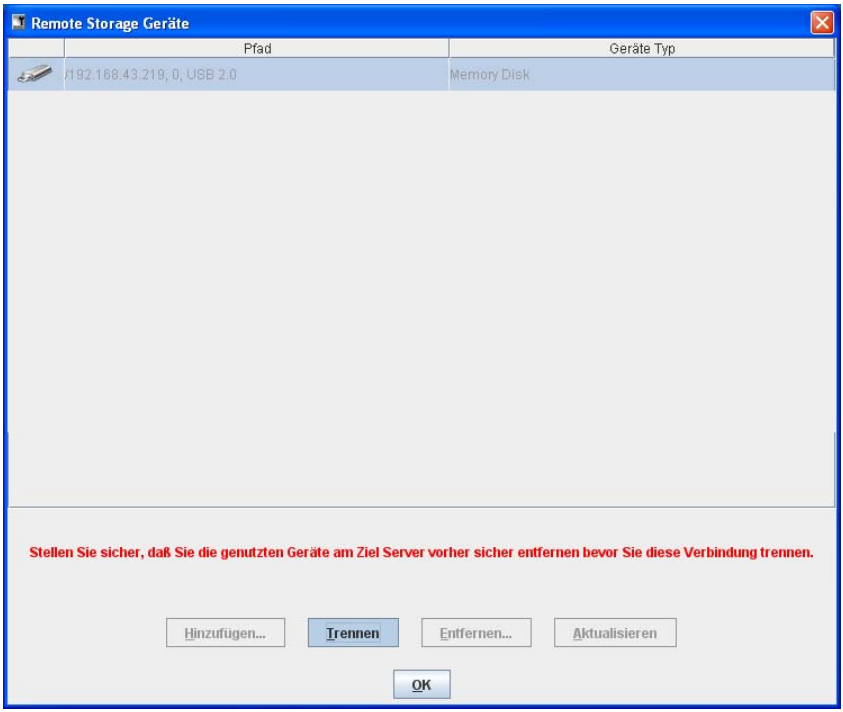


Bild 58: Dialog Remote Storage Geräte: Remote Storage-Verbindungen trennen

► Führen Sie ein „Sicheres Trennen“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.

► Klicken Sie auf *Trennen*, um alle Remote Storage-Verbindungen zu trennen.

6.1.5 Speichermedien entfernen

Aus der Liste der für Remote Storage bereitgestellten Speichermedien entfernen Sie ein Speichermedium wie folgt:

► Öffnen Sie den Dialog *Remote Storage Geräte* (siehe Abschnitt "Remote Storage starten" auf Seite 120).

Die Liste der für Remote Storage bereitgestellten Speichermedien wird angezeigt (Beispiel Windows):

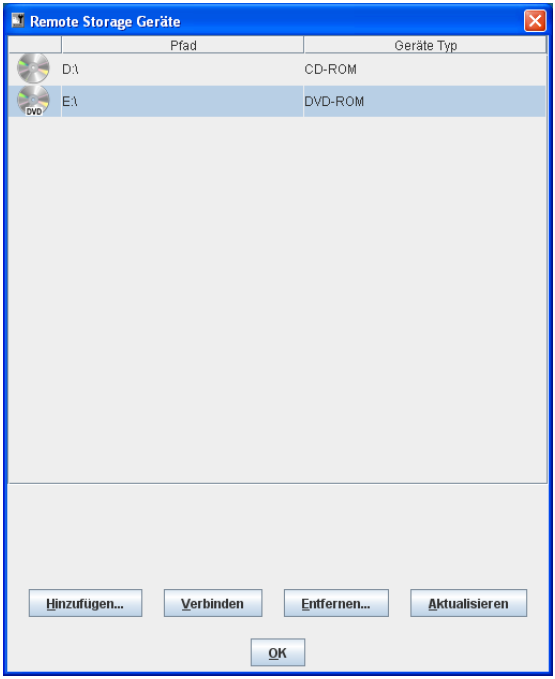


Bild 59: Dialog Remote Storage Geräte: Remote Storage Speichermedium entfernen

► Markieren Sie das Speichermedium, das Sie entfernen wollen.

► Klicken Sie auf *Entfernen...*, um das Speichermedium zu entfernen.

6.2 Remote Storage via Remote Storage Server bereitstellen

Mithilfe eines Remote Storage Servers können Sie für beliebige via iRMC S2/S3 administrierbare PRIMERGY Server in Ihrem Netz eine Image-Datei (Image File, ISO/NRG Abbild) als Remote Storage zur Verfügung stellen. Diese Image-Datei können Sie verwenden, um vom Remote-Arbeitsplatz aus einen oder mehrere PRIMERGY Server zu booten (siehe Kapitel "Remote-Installation des Betriebssystems via iRMC S2/S3" auf Seite 385).

Remote Storage Server ist für Windows-Systeme verfügbar

Der Remote Storage Server ist jeweils in einer 32-bit- und einer 64-bit-Variante für Windows verfügbar. Auf 64 bit-Systemen darf nicht gleichzeitig die 32 bit- und 64 bit-Version des Remote Storage Servers installiert sein.

Sie finden die einzelnen Varianten des Remote Storage Servers auf Ihrer ServerView Suite DVD 1 unter *SVSoftware\Software\RemoteView\iRMC*.

ISO-Abbild (ISO Image) dem PRIMERGY Server via Remote Storage zugänglich machen

Damit Ihr PRIMERGY Server die vom Remote Storage Server bereitgestellte Image-Datei nutzen kann, müssen folgende Voraussetzungen erfüllt sein:

– Der Remote Storage Server ist installiert (siehe Seite 134).

– Der Remote Storage Server ist gestartet (siehe Seite 139).

– Der iRMC S2/S3 des verwalteten Servers ist mit dem Remote Storage Server verbunden (siehe Seite 324).

WinPE 2.x-basierte ISO-Abbilder (ISO Images) booten

Das Booten eines WinPE 2.x-basierten ISO-Image (z.B. Windows Server 2008 und ServerView Installation Manager) setzt einen PRIMERGY Server mit iRMC S2/S3 und Firmware Version ≥ 3.60A voraus.

6.2.1 Remote Storage Server installieren

Die Installationsprogramme *RemoteStorageServer_Installer32.exe* und *RemoteStorageServer_Installer64.exe* zur Installation des Remote Storage Servers finden Sie auf der ServerView Suite DVD 1 unter *SVSoftware\Software\RemoteView\iRMC\Widows_32* bzw. *SVSoftware\Software\RemoteView\iRMC\Widows_x64*.

Nach erfolgreicher Installation enthält Ihr Installationsverzeichnis u.a. die Datei *RemoteStorageServer.exe*.

6.2.2 Ausführungsmodi des Remote Storage Servers

Den Remote Storage Server können Sie wahlweise in folgenden Modi ausführen:

– als Service im Hintergrund

– als eigenständiges (stand-alone) Programm

Den Ausführungsmodus des Remote Storage Servers konfigurieren Sie über eine grafische Bedienoberfläche (siehe Seite 136).

Remote Storage Server als Service ausführen

Folgende Punkte sind zu beachten:

– Die Image-Datei kann wahlweise auf einem Rechner im Netz oder auf dem Rechner liegen, auf dem der Remote Storage Server läuft.

  Falls die Image-Datei nicht auf dem Rechner liegt, auf dem der Remote Storage Server läuft, müssen Sie den Pfad der Image-Datei in UNC-Notation angeben. Ferner benötigen Sie eine Benutzerkennung mit Zugriffsberechtigung auf die Image-Datei.

– Beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, wird der Remote Storage Server automatisch gestartet. Der Remote Storage Server wird dann solange ausgeführt, bis er explizit beendet oder der Rechner heruntergefahren wird.

– Beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, ist die Image-Datei automatisch verfügbar.

Remote Storage Server als eigenständiges Programm ausführen

Folgende Punkte sind zu beachten:

– Die Image-Datei (ISO/NRG Abbild) darf lokal auf dem Remote Storage Server oder auf einem zugeordneten Netzlaufwerk liegen.

– Beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, müssen Sie die Image-Datei „von Hand“ starten.

6.2.3 Remote Storage Server konfigurieren, starten und beenden

Den Remote Storage Server konfigurieren, starten und beenden Sie über eine grafische Bedienoberfläche (GUI).

Grafische Bedienoberfläche des Remote Storage Servers aufrufen

Die grafische Bedienoberfläche des Remote Storage Servers rufen Sie wie folgt auf:

- Wählen Sie *Start - Alle Programme - Fujitsu RemoteStorageServer - Remote Storage Server*.

  Die grafische Bedienoberfläche des Remote Storage Servers wird angezeigt:

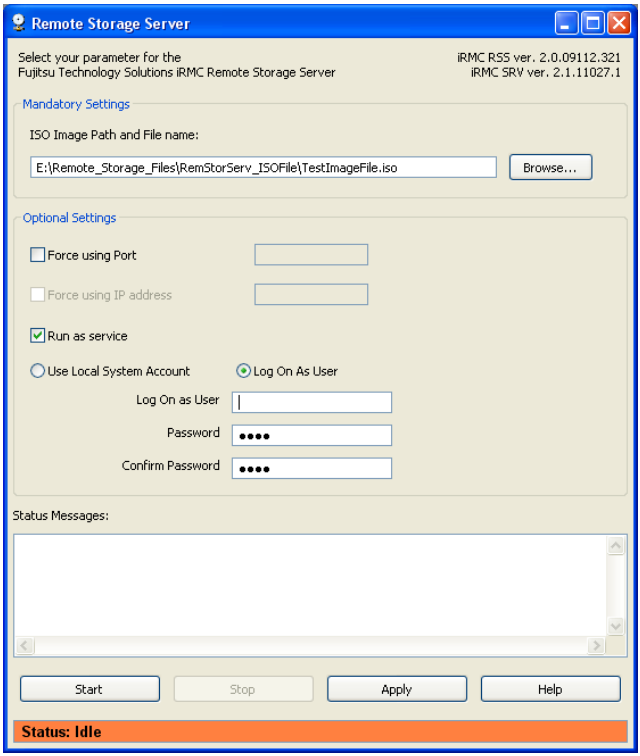


Bild 60: Grafische Bedienoberfläche des Remote Storage Servers (hier im Status „Idle“)

Remote Storage Server konfigurieren

Die Konfiguration setzt voraus, dass sich der Remote Storage Server im Status „idle“ befindet, also nicht ausgeführt wird.

Über die grafische Oberfläche spezifizieren Sie das als Remote Storage zur Verfügung gestellte Image-Datei sowie weitere Parameter:

ISO Image Path and Filename:

- Tragen Sie Pfad und Namen der Image-Datei direkt im Eingabefeld ein.

  oder:

- Klicken Sie auf die Schaltfläche *Browse...* und selektieren Sie in dem sich daraufhin öffnenden Dialog *Choose a file* die gewünschte Image-Datei per Navigieren und Bestätigungsdialog.

  Falls der Remote Storage Server als Service ausgeführt werden soll (siehe Option *Run as Service* auf Seite 138) und die Image-Datei auf einem Rechner im Netz liegt, müssen Sie den Pfad der Image-Datei in UNC-Notation spezifizieren. Stellen sie außerdem sicher, dass die unter *Log On As User* (siehe Seite 138) angegebene Benutzerkennung gültig ist und Zugriffsberechtigung für die freigegebene Netzwerk-Ressource besitzt, auf der die Image-Datei liegt.

Force Using Port

Wenn Sie für den Remote Storage Port des iRMC S2/S3 eine von der Default-Portnummer (5901) abweichende Portnummer konfiguriert haben (siehe Seite 255), müssen Sie diese Option aktivieren und im zugehörigen Eingabefeld die konfigurierte Portnummer eintragen.

Force Using IP Address

Falls der Rechner, auf dem der Remote Storage Server ausgeführt wird, über mehr als einen LAN-Anschluss verfügt:
Hier können Sie die IP-Adresse des LAN-Anschlusses angeben, der für den Remote Storage Server verwendet werden soll, wenn dieser als Service ausgeführt wird.
Standardmäßig verwendet der Remote Storage Server den ersten gefundenen LAN-Anschluss.

Run as Service

Aktivieren Sie diese Option, wenn der Remote Storage Server als Service im Hintergrund ausgeführt werden soll (siehe Seite 135).

► Wählen Sie eine der beiden folgenden Optionen:

Use Local System Account

Der Remote Storage Server wird als Service unter der lokalen Systemkennung ausgeführt.

Die Image-Datei (ISO/NRG Abbild) muss in diesem Fall auf einem lokalen Laufwerk liegen.

Log On As User

Der Remote Storage Server wird als Service unter der Benutzerkennung ausgeführt, die Sie in den nachfolgenden Eingabefeldern spezifizieren.

Spezifizieren Sie den Benutzernamen in der Form:

– Für lokale Benutzer: *.\Logon-Name*

– Für Domänen-Benutzer:

DOMAIN\LogOnName
oder
LogOnName@DOMAIN<mailto:LogOnName@DOMAIN>

Bei aktivierter Option *Log On As User* kann die Image-Datei (ISO/NRG Image) auf einem Netzlaufwerk liegen. In diesem Fall muss die angegebene Benutzerkennung Zugriffsrechte auf das Netzlaufwerk besitzen, auf dem die Image-Datei liegt. Außerdem müssen Sie den Pfad der Image-Datei in UNC-Notation spezifizieren (siehe Eingabefeld *ISO Image Path or Filename* auf Seite 137).

► Klicken Sie auf die Schaltfläche *Apply*, um Ihre Einstellungen zu aktivieren.

Remote Storage Server starten

► Klicken Sie auf die Schaltfläche *Start*, um den Remote Storage Server als Service oder als eigenständiges Programm zu starten:

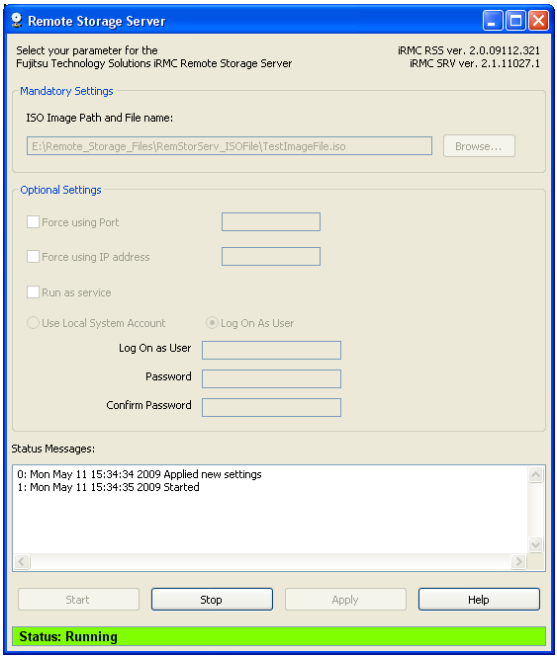


Bild 61: Remote Storage Server wird ausgeführt (Status „Running“)

Status Messages:

Hier werden die protokollierten Ausführungsstatus des Remote Storage Servers angezeigt.

Wenn der Ausführungsmodus *Run as service* konfiguriert ist (siehe Seite 138), wird der Remote Storage Server beim Booten des Rechners, auf dem der Remote Storage Server installiert ist, automatisch gestartet.

Die Ausführung des Remote Storage Servers wird bei Beenden der grafischen Bedienoberfläche nicht automatisch abgebrochen.

Remote Storage Server beenden

► Klicken Sie auf die Schaltfläche *Stop*, um die Ausführung des Remote Storage Servers zu beenden.

7 iRMC S2/S3-Web-Oberfläche

Der iRMC S2/S3 verfügt nicht nur über ein eigenes Betriebssystem, sondern fungiert auch als Web-Server und bietet eine eigene Web-Oberfläche. Dabei können Sie wählen, ob Sie sich die Menüs und Dialoge der iRMC S2/S3-Web-Oberfläche in deutscher, englischer oder japanischer Sprache anzeigen lassen möchten.

Bei der Eingabe von Werten an der iRMC S2/S3-Web-Oberfläche erhalten Sie in vielen Fällen zusätzliche Unterstützung in Form von Tooltipps.

Die im Folgenden beschriebene Software basiert zum Teil auf den Arbeiten der Independent JPEG Group.

7.1 An der iRMC S2/S3-Web-Oberfläche anmelden

► Öffnen Sie am Remote-Arbeitsplatz einen Web-Browser und geben Sie den (konfigurierten) DNS-Namen (siehe Seite 256) oder die IP-Adresse des iRMC S2/S3 ein.

Je nachdem, ob für den iRMC S2/S3 der LDAP-Zugriff auf einen Verzeichnisdienst (Directory Service) konfiguriert ist (Option *LDAP aktiviert*, siehe Seite 283), werden unterschiedliche Anmeldebildschirme angezeigt:

Falls kein Anmeldebildschirm angezeigt wird, überprüfen Sie die LAN-Verbindung (siehe Abschnitt "LAN-Schnittstelle testen" auf Seite 49).

– LDAP-Zugriff des iRMC S2/S3 auf den Verzeichnisdienst ist nicht konfiguriert (Option *LDAP aktiviert* ist nicht aktiviert) und Option *SSL Anmeldung immer aktiv* (siehe Seite 283) ist nicht aktiviert:

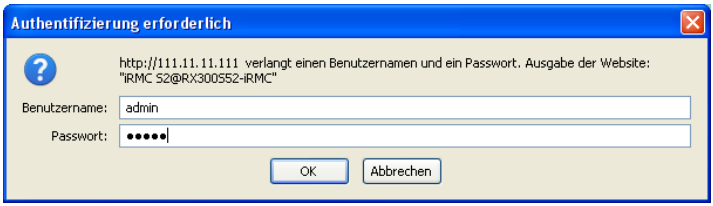


Bild 62: Anmeldebildschirm der iRMC S2/S3-Web-Oberfläche (LDAP-Zugriff nicht konfiguriert und Option „SSL Anmeldung immer aktiv“ ist nicht gewählt).

► Geben Sie die Daten der Standard-Administratorkennung ein:

Benutzername: admin

Kennwort: admin

Für *Benutzename* und *Kennwort* wird zwischen Groß- und Kleinschreibung unterschieden. Es wird empfohlen, wenn Sie sich angemeldet haben, aus Sicherheitsgründen eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort der Kennung zu ändern (siehe unter "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 275).

► Um zu bestätigen, klicken Sie auf die Schaltfläche *OK*.

– LDAP-Zugriff des iRMC S2/S3 auf den Verzeichnisdienst ist konfiguriert (Option *LDAP aktiviert* ist aktiviert) oder Option *SSL Anmeldung immer aktiv* ist aktiviert:

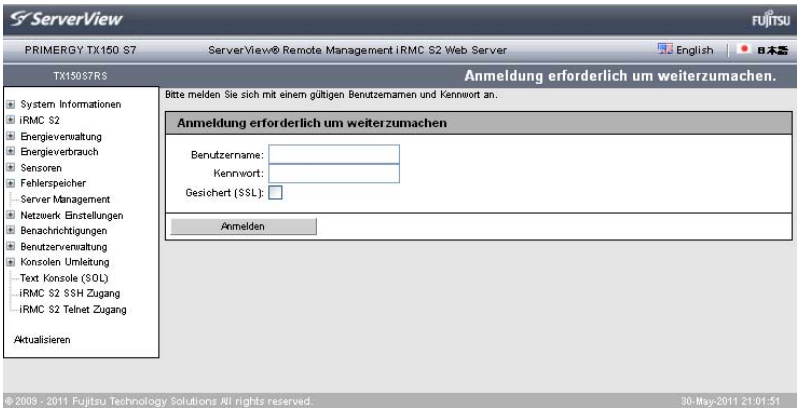


Bild 63: Anmeldebildschirm der iRMC S2/S3-Web-Oberfläche (LDAP-Zugriff konfiguriert)

Benutzname und Kennwort werden immer SSL-gesichert übertragen. Wenn Sie die Option *Gesichert (SSL)* aktivieren, erfolgt die gesamte Kommunikation zwischen Web-Browser und iRMC S2/S3 über HTTPS.

► Geben Sie die Daten der Standard-Administratorkennung ein:

Benutzername: admin

Kennwort: admin

Es wird empfohlen, wenn Sie sich angemeldet haben, aus Sicherheitsgründen eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort der Kennung zu ändern (siehe unter "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 275).

► Um zu bestätigen, klicken Sie auf die Schaltfläche *Anmelden*.

Die iRMC S2/S3-Web-Oberfläche öffnet sich, die Seite *System Überblick (*siehe Seite 152) wird angezeigt.

7.2 Erforderliche Benutzerberechtigungen

Tabelle 4 gibt einen Überblick, welche Berechtigungen zur Nutzung der einzelnen an der iRMC S2/S3-Web-Oberfläche angebotenen Funktionen erforderlich sind.

Funktion an iRMC S2/S3-Web-Oberfläche	Zulässig mit IPMI Privilege Level				Zulässig mit			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
Seite *System Überblick* öffnen.	X	X	X	X				
Identifizierungs-LED ein-/ausschalten.	X	X	X	X				
Inventar Information Konfiguration setzen.						X		
Betriebssystem Information editieren[1)]						X		
Seite *Sytem Komponenten Information* öffnen.	X	X	X	X				
Fehlerzähler zurücksetzen						X		
SPD Daten anzeigen.	X	X	X	X				
Seite *BIOS Parameter und Einstellungen sichern/ wiederherstellen* öffnen.[2)]	X	X	X	X				
Seite *BIOS Parameter und Einstellungen sichern/ wiederherstellen* bearbeiten.[2)]	X	X						
Seite *BIOS Einstellungen flashen* öffnen.[2)]	X	X	X	X				
BIOS aktualisieren (flashen).[2)]	X	X						
Seite *iRMC S2/S3 Informationen* öffnen.	X	X	X	X				
iRMC S2/S3 neu starten ausführen.	X	X						
Lizenzschlüssel auf den iRMC S2/S3 laden.						X		

Tabelle 4: Berechtigungen zur Nutzung der iRMC S2/S3-Web-Oberfläche

Funktion an iRMC S2/S3-Web-Oberfläche	Zulässig mit IPMI Privilege Level				Zulässig mit			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
Weitere iRMC S2/S3 Optionen setzen.						X		
Seite *RMC S2/S3 FW Einstellungen abspeich.ern* öffnen					X	X		
Benutzer Einstellungen wählen.					X			
Alle anderen Firmware Einstellungen wählen.						X		
iRMC S2/S3 Firmware Einstellungen in ServerView WinSCU XML Format importieren					X	X		
Seite *Zertifikat Austausch* öffnen und bearbeiten.						X		
Seite *Selbstign. RSA Zertifikat erzeugen* öffnen u. bearb.						X		
Seite *iRMC S2/S3 Aktualisierung* öffnen.	X	X	X	X				
Firmware-Selektor setzen.	X	X						
Firmware Aktualisierung aus einer Datei ausführen						X		
Firmware via TFTP aktualisieren (*iRMC S2/S3 TFTP...*)						X		
Seite *Ein-/Ausschalten* öffnen.	X	X	X	X				
Systemstart Optionen ändern.						X		
Ein-/Ausschalten und Neustart anwenden.	X	X	X					
Seite *Energieverwaltung Optionen* öffn./bearb.						X		
Seite *Netzteil Information* öffnen.	X	X	X	X				
Seite *Konfiguration der Enerergieverbrauchssteuerung* öffnen und bearbeiten.						X		
Seite *Akt. System Enerergieverbrauch* öffnen/bearb. [2)]						X		
Seite *Energieverbrauch Verlauf* öffnen/bearbeiten [2)]						X		

Tabelle 4: Berechtigungen zur Nutzung der iRMC S2/S3-Web-Oberfläche

Funktion an iRMC S2/S3-Web-Oberfläche	Zulässig mit IPMI Privilege Level				Zulässig mit			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
Seite *Lüfter* öffnen.	X	X	X	X				
Lüfterüberprüf. starten (Gruppe *Lüfter Überprüfung*).	X	X	X	X				
Lüftertest Uhrzeit setzen (Gruppe *Lüfter Überprüfung*).						X		
Lüftertest aktiviert setzen (Gruppe *System Lüfter*).						X		
Aktion bei Lüfterfehler / *Ausschalt Verzögerung* setzen.						X		

Tabelle 4: Berechtigungen zur Nutzung der iRMC S2/S3-Web-Oberfläche

Funktion an iRMC S2/S3-Web-Oberfläche	Zulässig mit IPMI Privilege Level				Zulässig mit			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
Seite *Temperatur* öffnen.	X	X	X	X				
Aktion bei kritischer Temperatur festlegen.						X		
Seite *Spannungen* öffnen.	X	X	X	X				
Seite *Netzteil* öffnen.	X	X	X	X				
Konfiguration der Stromversorgung Reundanz ausführen.						X		
Seite *Komponenten Status* öffnen.	X	X	X	X				
Seite *IPMI Fehlerliste* öffnen.	X	X	X	X				
Fehlerspeicher löschen.	X	X	X					
Fehlerliste speichern	X	X	X	X				
Fehlergewichte für Fehlerliste festlegen.	X	X	X	X				
Seite *Interner Ereignis Speicher Information* öffnen.	X	X						
Ereignisspeicher löschen.	X	X						
Interne Ereignisliste speichern	X	X						
Seite *Fehlerspeicher Konfiguration* öffnen.	X	X	X	X				
Fehlerspeicher konfigurieren.						X		
Fehlergewichte für interne Ereignisliste festlegen.						X		
Seite *Server Management Info.* öffnen und bearbeiten.						X		
Seite *Netzwerk Schnittstelle* öffnen und bearbeiten.						X		
Seite *Ports und Netzwerk Dienste* öffnen und bearb.						X		
Seite *DNS Konfiguration* öffnen und bearbeiten.						X		
Seite *SNMP TRAP Benachrichtigung* öffnen und bearb.						X		

Tabelle 4: Berechtigungen zur Nutzung der iRMC S2/S3-Web-Oberfläche

Funktion an iRMC S2/S3-Web-Oberfläche	Zulässig mit IPMI Privilege Level				Zulässig mit			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
Seite *Serielle / Modem Benachricht.* öffnen und bearb.						X		
Seite *E-Mail Benachrichtigung* öffnen und bearbeiten.						X		
Seite *Benutzer Verwaltung* öffnen und bearbeiten.					X			
Seite *Verzeichnisdienst Konfiguration* öffnen und bearb.						X		
Seite *CAS Konfiguration* öffnen					X	X		
CAS Allgemeine Konfiguration bearbeiten						X		
CAS Benutzer Privileg und Berechtigungen bearbeiten					X			
Seite *BIOS Text Konsole* öffnen.	X	X	X	X				
BIOS Konsolen Umleitung Optionen verändern.						X		
Start Video Umleitung durchführen.	X	X	X	X				
Logon im Fenster für Power-Mgmt. u. Text-Kons.-Uml.	X	X						
Text-Konsolen-Umleitung starten (*Enter Console*).	X	X						
Seite *Graf. Konsolen Umleitung* öffnen und bearbeiten.							X	
Seite *Remote Storage* öffnen und bearbeiten.								X
iRMC S2/S3 SSH Zugang starten	X	X	X	X				
SSH-Zugang	X	X	X	X				
iRMC S2/S3 Telnet Zugang starten	X	X	X	X				
Telnet-Zugang	X	X	X	X				

[1] Aktion ist nur möglich, wenn keine ServerView-Agenten ausgeführt werden.

[2] Funktionalität wird nicht von allen PRIMERGY Servern unterstützt.

Tabelle 4: Berechtigungen zur Nutzung der iRMC S2/S3-Web-Oberfläche

7.3 Aufbau der Bedienoberfläche

Die Bedienoberfläche der iRMC S2/S3-Web-Schnittstelle ist wie folgt aufgebaut:

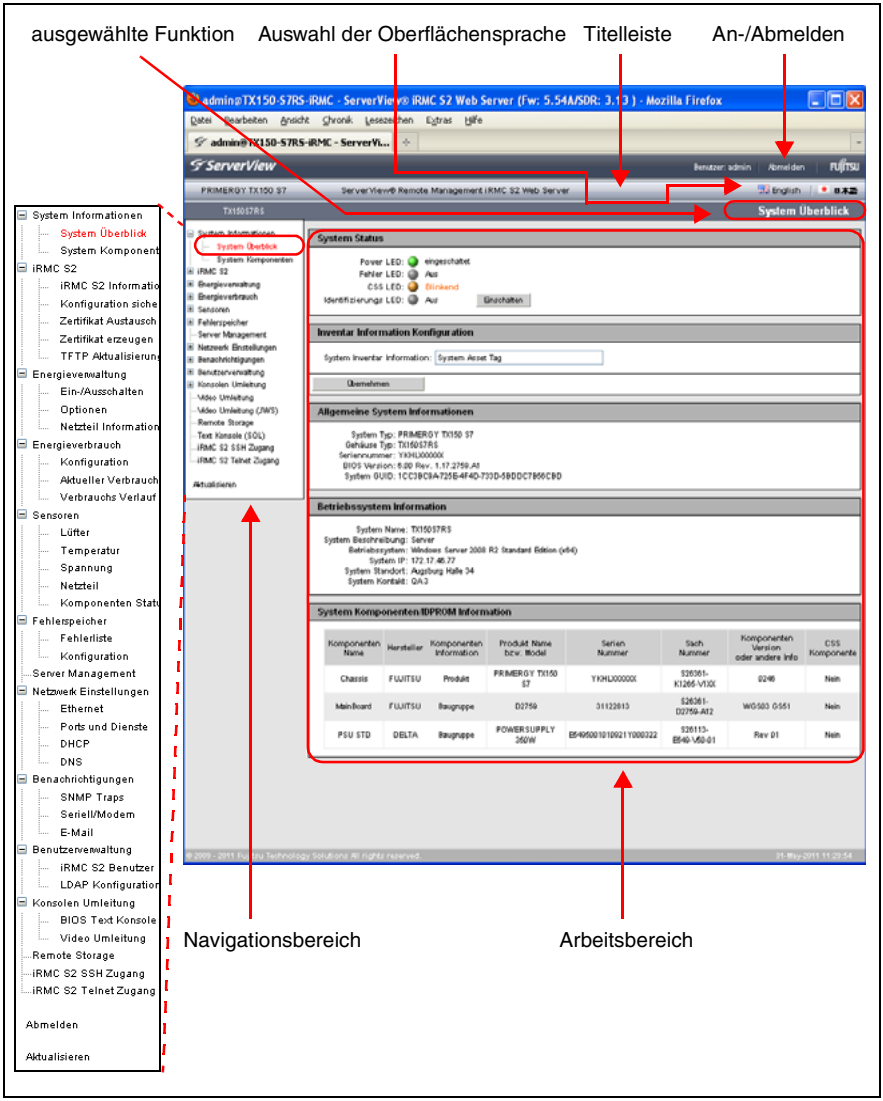


Bild 64: Aufbau der Bedienoberfläche der iRMC S2/S3-Web-Oberfläche

Landessprache für die iRMC S2/S3-Web-Oberfläche auswählen

In der schwarzen Leiste oberhalb des Arbeitsbereichs finden Sie rechts ein Flaggensymbol. Durch Klicken auf dieses Symbol wählen Sie die Landessprache (Deutsch / Englisch / Japanisch) für die Anzeige von Navigationsbereich, Menüs und Dialogen der iRMC S2/S3-Web-Oberfläche.

Navigationsbereich

Der Navigationsbereich enthält den Menübaum, dessen Knoten die Verweise auf die einzelnen iRMC S2/S3-Funktionen aufgabenorientiert zusammenfassen. Wenn Sie einen dieser Verweise anklicken (in Bild 64: *System Überblick*), wird der Verweis aktiviert und angezeigt wird der zur Funktion gehörige Arbeitsbereich mit Ausgaben, Feldern, Optionen, Verweisen und Schaltflächen.

Unterhalb der Verweise zu den einzelnen iRMC S2/S3-Funktionen finden Sie die Verweise *Abmelden* und *Aktualisieren*:

- Mit *Abmelden* können Sie über einen Bestätigungsdialog die aktuelle iRMC S2/S3-Session beenden. Je nachdem, ob für den iRMC S2/S3 der LDAP-Zugriff auf einen Verzeichnisdienst (Directory Service) konfiguriert ist (Option *LDAP aktiviert*, siehe Seite 283), werden nach Beendigung der Session unterschiedliche Anmelde-Seiten angezeigt:
  - Falls der LDAP-Zugriff des iRMC S2/S3 auf den Verzeichnisdienst nicht konfiguriert ist (Option *LDAP aktiviert* ist nicht aktiviert) und auch die Option *SSL Anmeldung immer aktiv* (siehe Seite 283) deaktiviert ist, wird die folgende Anmelde-Seite angezeigt:

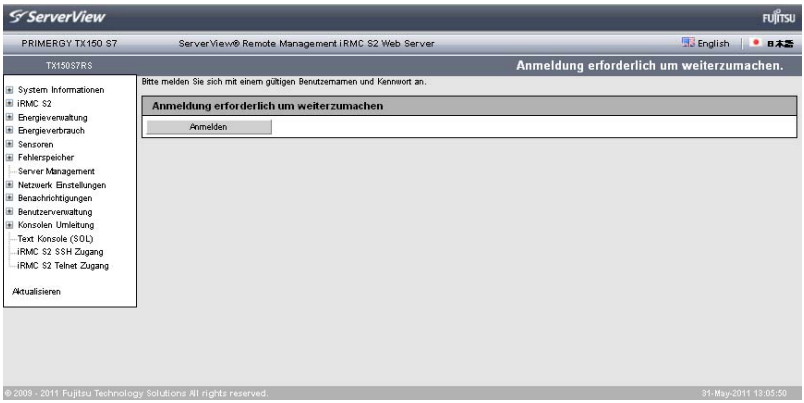


Bild 65: Anmelde-Seite (nach Abmelden)

Durch Klicken auf die Schaltfläche *Anmelden* gelangen Sie zur Anmelde-Seite der iRMC S2/S3-Web-Oberfläche, über den Sie sich erneut anmelden können (siehe Bild 62 auf Seite 142).

– Falls der LDAP-Zugriff des iRMC S2/S3 auf den Verzeichnisdienst konfiguriert ist (Option *LDAP aktiviert* ist aktiviert) oder die Option *SSL Anmeldung immer aktiv* aktiviert ist, wird der entsprechende Anmelde-Seite angezeigt (siehe Bild 63 auf Seite 143).

- Mit *Aktualisieren* aktualisieren Sie die Anzeige der iRMC S2/S3-Web-Oberfläche.

  Optional können Sie die automatische periodische Aktualisierung der Anzeige konfigurieren (siehe "Automatisch aktualisieren" auf Seite 253).

7.4 System Informationen - Informationen zum Server

Der Eintrag *System Informationen* enthält die Verweise auf folgende Seiten:

– "System Überblick - Allgemeine Informationen zum Server" auf Seite 153

– "System Komponenten Information - Informationen zu den Server-Komponenten" auf Seite 158

7.4.1 System Überblick - Allgemeine Informationen zum Server

Die Seite *System Überblick* liefert folgende Informationen:

- System-Status,
- System (allgemeine Informationen),
- Betriebssystem des verwalteten Servers,
- Systemkomponenten / IDPROM,
- Gesamt-Energieverbrauch des verwalteten Servers.

Außerdem können Sie auf der Seite *System Überblick* ein von Ihnen gewähltes Bestandskennzeichen („kundenspezifisches Asset Tag“) für den verwalteten Server eintragen.

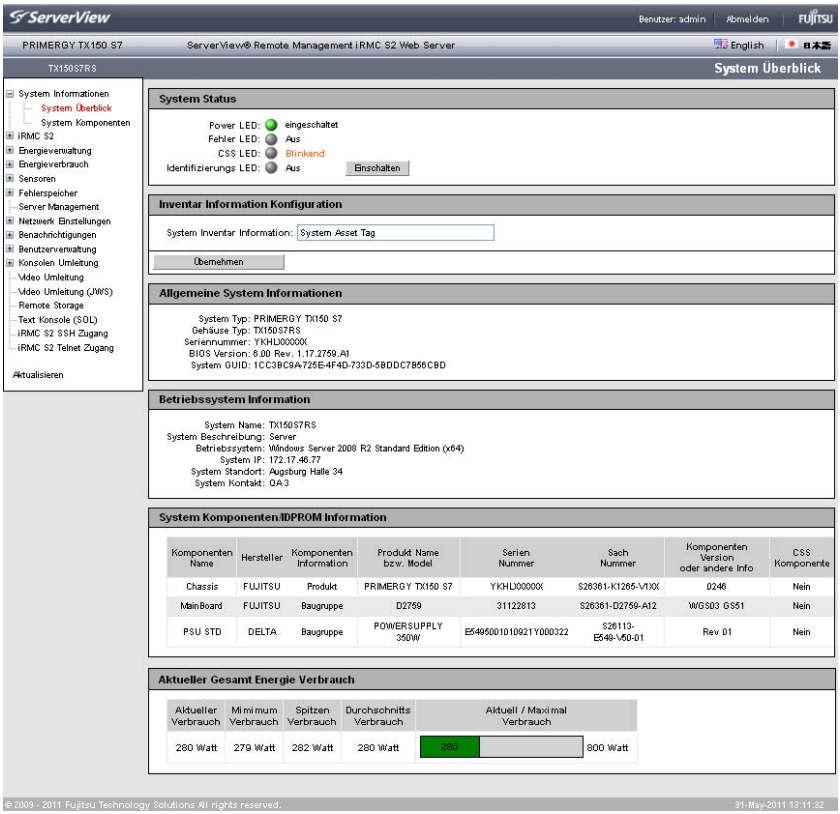


Bild 66: Seite System Überblick

System Status

Unter *System Status* werden Sie über die CSS-/Globale Fehler-Anzeige am PRIMERGY Server informiert. Außerdem können Sie die PRIMERGY Identifizierungs-LED ein- und ausschalten.

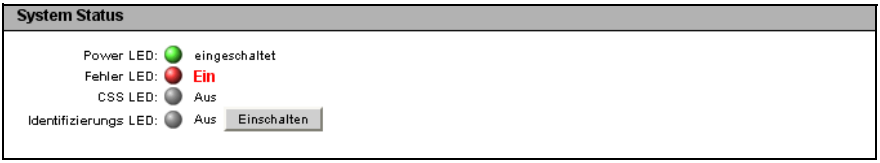


Bild 67: Seite System Überblick - System Status

Power LED

Power-Zustand des Servers.
Folgende Status sind möglich:

- eingeschaltet: „Power ON“ (grün)
- Standbymodus: „Power ON“ (grün) und Hinweis „Standbymodus“.
- „Power OFF“ (orange)

Fehler LED

Informiert über Fehler-LED (Global Error-LED) am Server:

Anzeige (iRMC S2/S3)	Fehler-LED am Server	Status des Servers
Aus	Leuchtet nicht.	Es liegt kein kritisches Ereignis vor.
Ein	Leuchtet rot.	Prefailure-Ereignis für eine Nicht-CSS-Komponente.
Blinkend	Blinkt rot.	Kritisches Ereignis.

CSS LED

Informiert über CSS (Customer Self Service)-LED am Server:

Anzeige (iRMC S2/S3)	CSS-LED am Server	Status des Servers
Aus	Leuchtet nicht.	Der Server ist in Ordnung.
Ein	Leuchtet orange.	Prefailure-Ereignis für eine CSS-Komponente.
Blinkend	Blinkt orange.	Defekte CSS-Komponente.

Identifizierungs LED

Identifizierung des Servers.
Folgende Status sind möglich:

– eingeschaltet (grün)
– ausgeschaltet: (orange)

Einschalten / Ausschalten

Durch Klicken auf die alternierende Schaltfläche *Einschalten* / *Ausschalten* können Sie die Identifizierungs-LED ein- bzw. ausschalten.

Inventar Information Konfiguration

Unter *Inventar Information Konfiguration* können Sie ein von Ihnen gewähltes Bestandskennzeichen („kundenspezifisches Asset Tag“) für den verwalteten Server eintragen.

Mithilfe des kundspezifische Asset Tags können Sie dem Server eine von Ihnen gewählte Inventarnummer oder sonstige Identifikation geben.

In Windows-basierten Systemen wird dieses kundenspezifische Asset Tag automatisch in WMI (Windows Management Instrumentation) zur Verfügung gestellt und kann dann zur Auswertung durch anwendereigene Tools oder für eine Integration in Enterprise Management Systeme (wie z.B. CA Unicenter) verwendet werden.

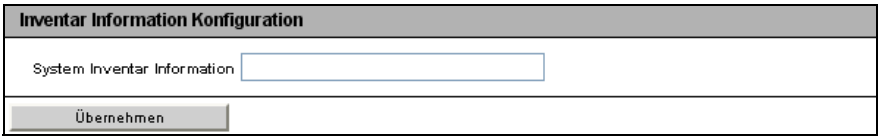


Bild 68: Seite System Überblick - System Status

Sytem Inventar Information

Hier können Sie das Bestandskennzeichen eingeben.

► Klicken Sie auf die Schaltfläche *Übernehmen,* um das Bestandskennzeichen zu übernehmen.

Allgemeine System Informationen

Unter *Allgemeine Sytem Informationen* sind Informationen zum verwalteten Server aufgelistet.

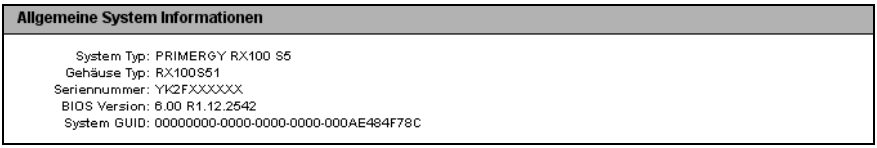


Bild 69: Seite System Überblick - Allgemeine System Informationen

Betriebssystem Information

Unter *Betriebssystem Information* sind Informationen zum Betriebssystem des verwalteten Servers aufgelistet.

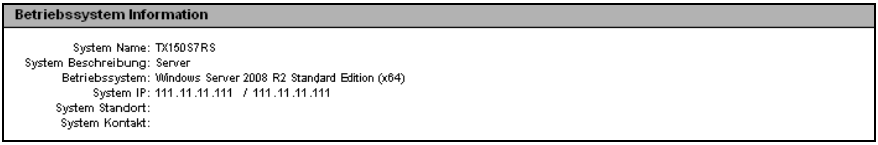


Bild 70: Seite System Überblick - Betriebssystem Information

Wenn keine ServerView-Agenten ausgeführt werden, können Sie die Felder *System Standort* und *System Kontakt* editieren, andernfalls können diese Felder nicht verändert werden.

Nach dem Start der ServerView-Agenten werden Ihre ursprünglichen Werte mit den von den Agenten automatisch ermittelten Werten überschrieben.

System Komponenten/IDPROM Information

Unter *Sytem Komponenten/IDPROM Information* sind Informationen zu den FRUs (**F**ield **R**eplaceable **U**nits) aufgelistet. FRUs sind Systemkomponenten, die freigegeben und aus dem System entfernt werden können. In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice)-Funktionalität unterstützt wird.

System Komponenten/IDPROM Information

Komponenten Name	Hersteller	Komponenten Information	Produkt Name bzw. Model	Serien Nummer	Sach Nummer	Komponenten Version oder andere Info	CSS Komponente
Chassis	FSC	Produkt	PRIMERGY RX100 S5	YK2FXXXXXX	S26361-K1160-VXXX	0225	Nein
MainBoard	FSC	Produkt	PRIMERGY RX100 S5	YK2Fxxxxxx	S26361-K1160-Vxxx	0225	Nein
MainBoard	FSC	Baugruppe	D2542	5554Y01001G746001C4J0A1	S26361-D2542-B10	WGS01 GS01	Nein
PSU	DELTA	Baugruppe	DPS-350UB A	AFDC0731000255	56.04350.111	S2	Nein

Bild 71: Seite System Überblick - System Komponenten/IDPROM Information

Aktueller Gesamt Energieverbrauch

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

Aktueller Gesamt Energieverbrauch

Aktueller Verbrauch	Mimimum Verbrauch	Spitzen Verbrauch	Durchschnitts Verbrauch	Aktuell / Maximal Verbrauch
280 Watt	279 Watt	282 Watt	280 Watt	280 / 800 Watt

Bild 72: Seite System Überblick - Aktueller Gesamt Energieverbrauch

Unter *Aktueller Gesamt Energieverbrauch* werden die Messwerte zum aktuellen, minimalen, maximalen sowie durchschnittlichen Energieverbrauch des verwalteten Servers im aktuellen Intervall angezeigt.

In einer grafischen Anzeige wird außerdem der aktuelle Energieverbrauch des Servers der maximal möglichen Leistungsaufnahme gegenübergestellt.

7.4.2 System Komponenten Information - Informationen zu den Server-Komponenten

Die Seite *System Komponenten Information* liefert Informationen zur CPU und den Hauptspeicher-Modulen. In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice)-Funktionalität unterstützt wird.

Die möglichen Status der Systemkomponenten werden durch folgende Status-Icons symbolisiert:

	OK: Der Zustand der Komponente ist in Ordnung.
	Der Steckplatz für die Komponente ist leer.
	Warnung: Der Zustand der Komponente hat sich verschlechtert.
	Fehler: Die Komponente hat einen Fehler.

Tabelle 5: Status der Systemkomponente

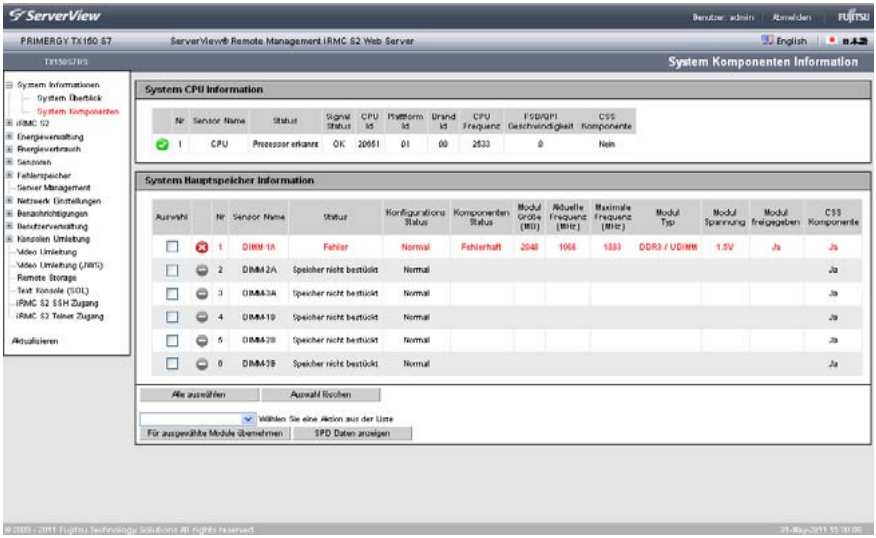


Bild 73: Seite System Komponenten Information (ohne SPD-Daten)

Bei PRIMERGY Servern mit TPM (Trusted Platform Module)-Unterstützung wird angezeigt, ob TPM aktiviert oder deaktiviert ist.

System CPU Information

Diese Gruppe informiert über Status, IDs, CSS-Eignung und Leistungsdaten der CPU(s) im verwalteten PRIMERGY Server.

System Hauptspeicher Information

Diese Gruppe informiert über Status, IDs, CSS-Eignung und Leistungsdaten der Hauptspeichermodule im verwalteten PRIMERGY Server.

Auswahl
: Hier können Sie einzelne Speichermodule auswählen, auf die die unter *Wählen Sie eine Aktion aus der Liste* gewählte Aktion ausgeführt werden soll.

Alle auswählen
: Wählt alle Speichermodule aus.

Auswahl löschen
: Löscht die Auswahl.

Wählen Sie eine Aktion aus der Liste

Aus dieser Liste können Sie eine Aktion auswählen, die auf die ausgewählten Speichermodule angewendet werden soll.

Das Rücksetzen des Fehlerzählers ist nicht möglich im Falle eines BX92x S3 ServerBlade. Beim iRMC S3 oder BX92x S3 ServerBlade ist es nicht mehr erforderlich, den Fehlerzähler explizit zurückzusetzen, da neue Module automatisch erkannt werden und der Fehlerzähler dabei auf 0 gesetzt wird.

Für ausgewählte Module übernehmen

Führt die gewählte Aktion auf die ausgewählten Speichermodule aus.

SPD Daten anzeigen / Keine SPD Daten anzeigen

Durch Klicken auf die alternierende Schaltfläche *SPD Daten anzeigen / Keine SPD Daten anzeigen* blenden Sie Hersteller-spezifische Angaben (**S**erial **P**resence **D**etect (SPD)-Daten) zu den einzelnen Speicherkomponenten ein- bzw. aus.

Die SPD-Daten einer Speicherkomponente sind auf einem in die Komponente integrierten EEPROM abgelegt und dienen der automatischen Erkennung dieser Speicherkomponente (RAM, DIMM) durch das BIOS.

7.5 BIOS-Einstellungen sichern/ wiederherstellen, BIOS aktualisieren

Der Eintrag *BIOS* enthält Links zu den folgenden Seiten:

– "BIOS-Parameter und -Einstellungen in Datei sichern / aus Datei wiederherstellen" auf Seite 161

– "BIOS aktualisieren via "Aktualisierung aus Datei" oder via TFTP" auf Seite 166

Diese Seiten werden nur dann angezeigt, wenn das BIOS des verwalteten Servers die entsprechenden funktionalen Anforderungen unterstützt.

7.5.1 BIOS-Parameter und -Einstellungen in Datei sichern / aus Datei wiederherstellen

Die Seite *BIOS Parameter und Einstellungen sichern/wiederherstellen* bietet Ihnen folgende Möglichkeiten:

– Einstellungen einzelner BIOS-Parameter im ServerView® WinSCU XML-Format sichern und die Sicherung in einer Datei speichern.

– Einstellungen einzelner BIOS-Parameter im ServerView® WinSCU XML-Format auf Basis einer Sicherungsdatei wiederherstellen.

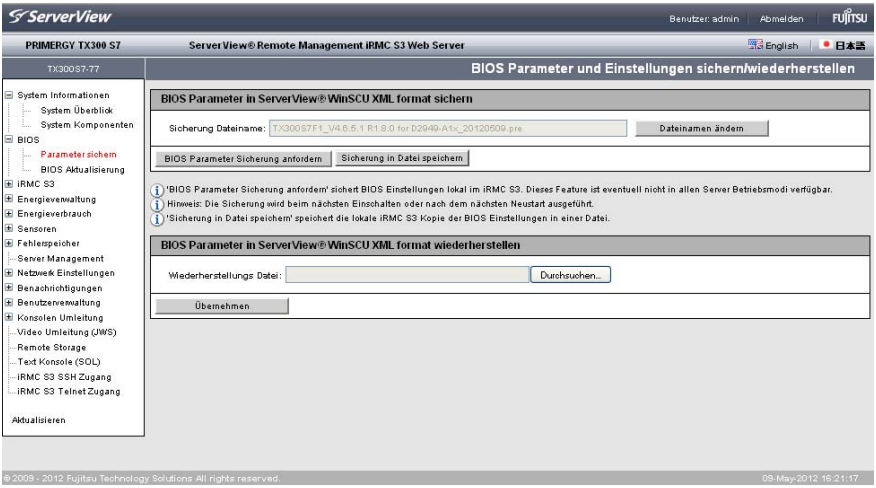


Bild 74: Seite BIOS Parameter und Einstellungen sichern/wiederherstellen

7.5.1.1 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format sichern

Mit der Gruppe *BIOS Parameter in ServerView® WinSCU XML format sichern* können Sie die Einstellungen einzelner BIOS parameter im ServerView® WinSCU XML sichern und die Sicherung in einer Datei speichern.

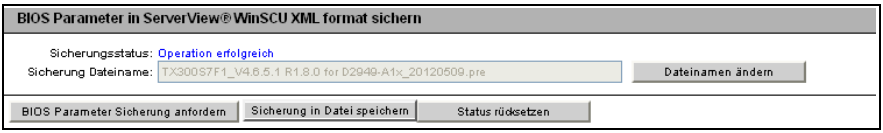


Bild 75: BIOS-Parameter im ServerView® WinSCU XML-Format sichern

Sicherungsstatus

Zeigt den Status des aktuellen Sicherungsprozesses an. Ein erfolgreicher Abschluss wird durch "Operation erfolgreich" angezeigt. Der *Sicherungsstatus* wird nur dann angezeigt, wenn die Sicherung gerade durchgeführt wird oder abgeschlossen ist.

Zum Löschen der Anzeige klicken Sie auf die Schaltfläche *Status zurücksetzen*, die nur dann vorhanden ist, wenn zurzeit ein Status angezeigt wird.

Status zurücksetzen

Löscht die unter *Sichrungsstatus* angezeigte Statusinformation. Diese Schaltfläche ist nur dann vorhanden, wenn zurzeit unter *Sicherrungsstatus* ein Status angezeigt wird.

Sicherung Dateiname

Dieses Eingabefeld ist standardmäßig deaktiviert ("ausgegraut"). Vorbelegt ist es mit dem vom iRMC S2/S3 dynamisch generierten Dateinamen.

Dateinamen ändern

Aktiviert das Feld *Sicherung Dateiname*, sodass Sie einen Dateinamen (*.pre*) Ihrer Wahl eingeben können.

Dateiname speichern

Sichert den geänderten Dateinamen, der ab sofort standardmäßig im Feld *Sicherung Dateiname* angezeigt wird.

BIOS Parameter Sicherung anfordern

Startet die Sicherung einzelner BIOS-Parameter-Einstellungen im ServerView® WinSCU XML format. Die Sicherung (mit dem im Feld *Sicherung Dateiname* angezeigten Namen) wird lokal am iRMC S2/S3 gespeichert.

Sobald der Sicherungsprozess gestartet ist, wird der aktuelle Prozessstatus unter *Sicherungsstatus* angezeigt.

Hinweise zum Sicherungsprozess:

- Während des Sicherungsprozesses sind alle Schaltflächen und Eingabefelder deaktiviert.
- Falls der Server ausgeschaltet ist, wird er automatisch eingeschaltet.
- Falls der Server eingeschaltet ist, ist ein Reboot erforderlich. Andernfalls verbleibt der Server im Zustand "Boot steht noch aus".
- Nach Abschluss des Sicherungsprozesses wird der Server ausgeschaltet.

Sicherung in Datei speichern

Öffnet einen Browser-Dialog, über den Sie die iRMC S2/S3-lokale Kopie der BIOS-Sicherungsdaten in eine Datei (<*beliebiger-name*>.*pr*e) sichern können.

Diese Schaltfläche wird nur dann angezeigt, wenn eine Sicherung einzelner BIOS-Parameter im ServerView® WinSCU XML-Format im lokalen Speicher des iRMC S2/S3 vorhanden ist.

7.5.1.2 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format wiederherstellen

Mit der Gruppe *BIOS Parameter in ServerView® WinSCU XML format wiederherstellen* können Sie die Einstellungen einzelner BIOS-Parameter im ServerView® WinSCU XML-Format auf Basis einer Sicherungsdatei wiederherstellen.

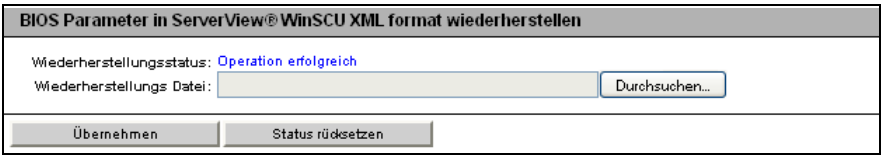


Bild 76: BIOS-Parameter im ServerView® WinSCU XML Format wiederherstellen

Wiederherstellungsstatustatus

Zeigt den Status des aktuellen Wiederherstellungsprozesses an. Ein erfolgreicher Abschluss wird durch "Operation erfolgreich" angezeigt. Der *Wiederherstellungsstatus* wird nur dann angezeigt, wenn die Wiederherstellung gerade durchgeführt wird oder abgeschlossen ist.

Zum Löschen der Anzeige klicken Sie auf die Schaltfläche *Status zurücksetzen*, die nur dann vorhanden ist, wenn zurzeit ein Status angezeigt wird.

Status rücksetzen

Löscht die unter *Wiederherstellungsstatus* angezeigte Statusinformation. Diese Schaltfläche ist nur dann vorhanden, wenn zurzeit unter *Wiederherstellungsstatus* ein Status angezeigt wird.

Wiederherstellungs Datei

Ein Klick ins Eingabefeld oder auf *Durchsuchen...* öffnet einen Browser-Dialog, über den Sie zu einer Datei (*.pre*) navigieren können, die eine Sicherung einzelner BIOS-Parameter im ServerView® WinSCU XML-Format enthält.

Übernehmen

Startet die Wiederherstellung einzelner BIOS-Parameter-Einstellungen auf Basis der im Feld *Wiederherstellungs Datei* spezifizierten Datei.

Sobald der Sicherungsprozess gestartet ist, wird der aktuelle Prozessstatus unter *Wiederherstellungsstatus* angezeigt.

Hinweise zum Wiederherstellungsprozess:

- Während des Wiederherstellungsprozesses sind alle Schaltflächen und Eingabefelder deaktiviert.
- Falls der Server ausgeschaltet ist, wird er automatisch eingeschaltet.
- Falls der Server eingeschaltet ist, ist ein Reboot erforderlich. Andernfalls verbleibt der Server im Zustand "Boot steht noch aus".
- Nach Abschluss des Sicherungsprozesses wird der Server ausgeschaltet.

7.5.2 BIOS aktualisieren via "Aktualisierung aus Datei" oder via TFTP

Die Seite *BIOS Einstellungen flashen* liefert Informationen zur aktuellen BIOS-Version auf dem verwalteten Server und ermöglicht es Ihnen, das BIOS via "Aktualisierung aus Datei" oder via TFTP zu aktualisieren.

Das geeignete BIOS-Image für Ihren PRIMERGY Server finden Sie auf der ServerView Suite DVD 1 oder zum Download unter:

http://support.ts.fujitsu.com/com/support/downloads.html

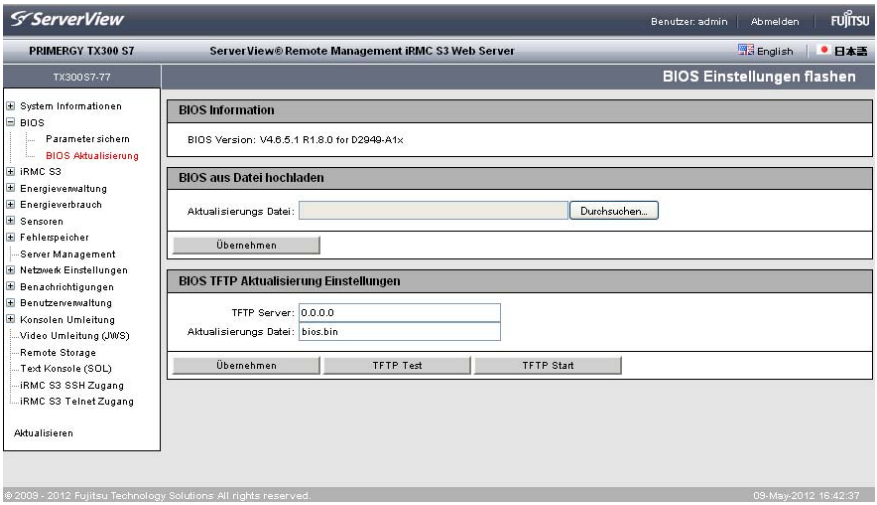


Bild 77: Seite BIOS Einstellungen flashen

BIOS aktualisieren ("flashen") - Ablauf und wichtige Hinweise

Der folgende Überblick gilt sowohl für die BIOS-Aktualisierung via "Aktualisierung aus Datei" als auch für die BIOS-Aktualisierung via TFTP.

Einzelheiten zum Starten der in diesem Überblick beschriebenen Schritte sind weiter unten in diesem Abschnitt beschrieben.

Während des kompletten Aktualisierungsprozesses wird der aktuelle Status in der Seite *BIOS Einstellungen flashen* angezeigt.

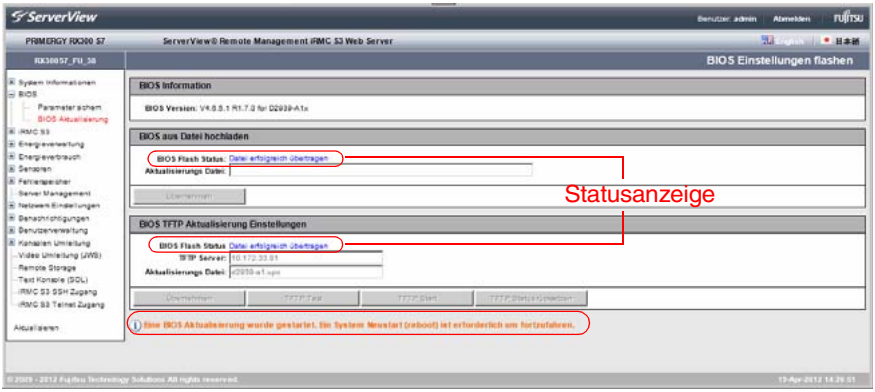


Bild 78: BIOS-Aktualisierung - (TFTP) Download erfolgreich abgeschlossen

Die BIOS-Aktualisierung umfass die folgenden Schritte:

1. Im ersten Schritt laden Sie die Aktualisierungsdatei herunter.

   Die Aktualisierungsdatei muss einen *UPC*-Datei sein.

   Nach dem Herunterladen der Aktualisierungsdatei geht es wie folgt weiter:

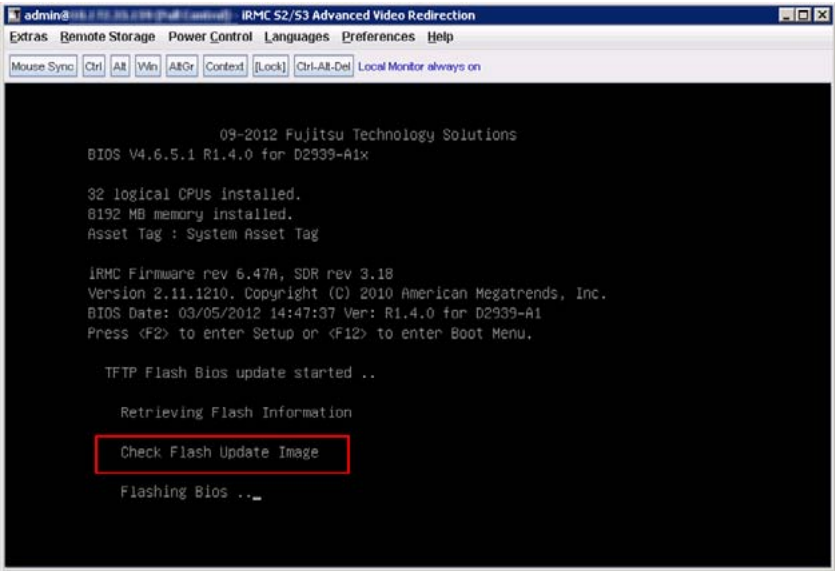
   – Falls der Server ausgeschaltet ist, wird er für den Aktualisierungsprozess automatisch eingeschaltet.

   – Falls der Server bereits eingeschaltet ist, müssen Sie den Server für den Aktualisierungsprozess neu starten.

   ACHTUNG!

   Falls gerade eine BIOS-Aktualisierung durchgeführt wird: Schalten Sie den Server **nicht** aus und führen Sie auch **keinen Neustart** durch.

2. Anschließend werden die Aktualisierungsdaten (Flash-Daten) in den Speicher übertragen. Die Statusanzeige informiert, wenn die Übertragung erfolgreich abgeschlossen ist.
3. Vor dem Start des eigentlichen Flash-Prozesses wird das Flash/ Aktualiserungs-Image geprüft.


admin@ iRMC S2/S3 Advanced Video Redirection
Extras Remote Storage Power Control Languages Preferences Help
Mouse Sync Ctrl Alt Win AltGr Context [Lock] Ctrl-Alt-Del Local Monitor always on
09-2012 Fujitsu Technology Solutions
BIOS V4.6.5.1 R1.4.0 for D2939-A1x
32 logical CPUs installed.
8192 MB memory installed.
Asset Tag : System Asset Tag
iRMC Firmware rev 6.47A, SDR rev 3.18
Version 2.11.1210. Copyright (C) 2010 American Megatrends, Inc.
BIOS Date: 03/05/2012 14:47:37 Ver: R1.4.0 for D2939-A1
Press <F2> to enter Setup or <F12> to enter Boot Menu.
TFTP Flash Bios update started ..
Retrieving Flash Information
Check Flash Update Image
Flashing Bios ..
Bild 79: BIOS aktualisieren - Update (Flash-Image) prüfen

4. Nach erfolgreicher Verifizierung des Flash/Aktualisierungs-Image wird der eigentliche Flash-Prozess gestartet. Die Statusanzeige informiert über den prozentualen Fortschritt des Flash-Prozesses.
5. Nach erfolgreichem Abschluss der BIOS-Aktualisierung schaltet sich der Server aus. Der folgende Eintrag wird in den Ereignisspeicher (System Event Log, SEL) geschrieben:

   `BIOS TFTP or HTTP/HTTPS flash OK`

BIOS Information

Diese Gruppe informiert über die aktuelle BIOS-Version auf dem verwalteten Server.

BIOS-Aktualisierung aus einer Datei

Mit der Gruppe *BIOS aus Datei hochladen* können Sie eine Online-Aktualisierung des BIOS auf dem verwalteten Server durchführen. Hierfür müssen Sie das aktuelle BIOS-Image in einer Datei bereitstellen.

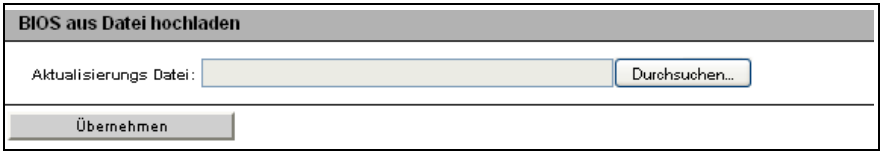


Bild 80: Seite BIOS Einstellungen flashen - BIOS aus Datei hochladen

Aktualisierungs Dateie

Datei, in der das BIOS-Image gespeichert ist.

Für die Ausführung der Funktion *BIOS aus Datei hochladen* ist das *UPC*-Format erforderlich.

Durchsuchen...

Öffnet den Datei-Browser, über den Sie zur Aktualisierungsdatei navigieren können.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren und die BIOS-Aktualisierung zu starten.

ACHTUNG!

Falls gerade eine BIOS-Aktualisierung durchgeführt wird: Schalten Sie den Server **nicht** aus und führen Sie auch **keinen Neustart** durch.

BIOS-Aktualisierung via TFTP

Mit der Gruppe *BIOS TFTP Aktualisierung Einstellungen* können Sie eine Online-Aktualisierung des BIOS auf dem verwalteten Server durchführen. Hierfür müssen Sie das aktuelle BIOS-Image in einer Datei auf einem TFTP-Server bereitstellen. Das BIOS wird aktualisiert, sobald TFTP gestartet ist.

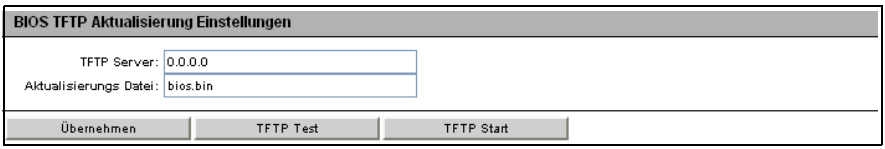


Bild 81: BIOS Update Settings page - BIOS TFTP Update Settings

TFTP Server

IP-Adresse oder DNS-Name des TFTP-Servers, auf dem die Datei mit dem BIOS-Image gespeichert ist.

Aktualisierungs Datei

Datei, inder das BIOS-Image gespeichert ist.

Für die Ausführung der Funktion *BIOS TFTP Aktualisierung Einstellungen* ist das *UPC*-Format erforderlich.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.
- Klicken Sie auf *TFTP Test*, um die Verbindung zum TFTP-Server zu testen.
- Klicken Sie auf *TFTP Start,* um die Datei mit dem BIOS-Image vom TFTP-Server herunterzuladen und die BIOS-Aktualisierung zu starten.

ACHTUNG!

Falls gerade eine BIOS-Aktualisierung durchgeführt wird: Schalten Sie den Server **nicht** aus und führen Sie auch **keinen Neustart** durch.

7.6 iRMC S2/S3 - Informationen, Firmware und Zertifikate

Der Eintrag *iRMC S2/S3* enthält Verweise auf die folgenden Seiten:

– "iRMC S2/S3 Informationen - Informationen zum iRMC S2/S3" auf Seite 172

– "iRMC S2/S3 Firmware Einstellungen abspeichern" auf Seite 176

– "Zertifikat Austausch - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden" auf Seite 178

– "Selbstsigniertes RSA Zertifikat erzeugen" auf Seite 185

– "iRMC S2/S3 Firmware Aktualisierung" auf Seite 187

7.6.1 iRMC S2/S3 Informationen - Informationen zum iRMC S2/S3

Die Seite *iRMC S2/S3 Informationen* bietet Ihnen folgende Möglichkeiten:

– Informationen zu Firmware- und SDRR-Version des iRMC S2/S3 einsehen, den Firmware-Selektor setzen und den iRMC S2/S3 neu starten.

– Informationen über aktive iRMC S2/S3-Sitzungen einsehen.

– Lizenzschlüssel (License Key) auf den iRMC S2/S3 laden.

– Einstellungen für das Layout der iRMC S2/S3-Web-Oberfläche festlegen

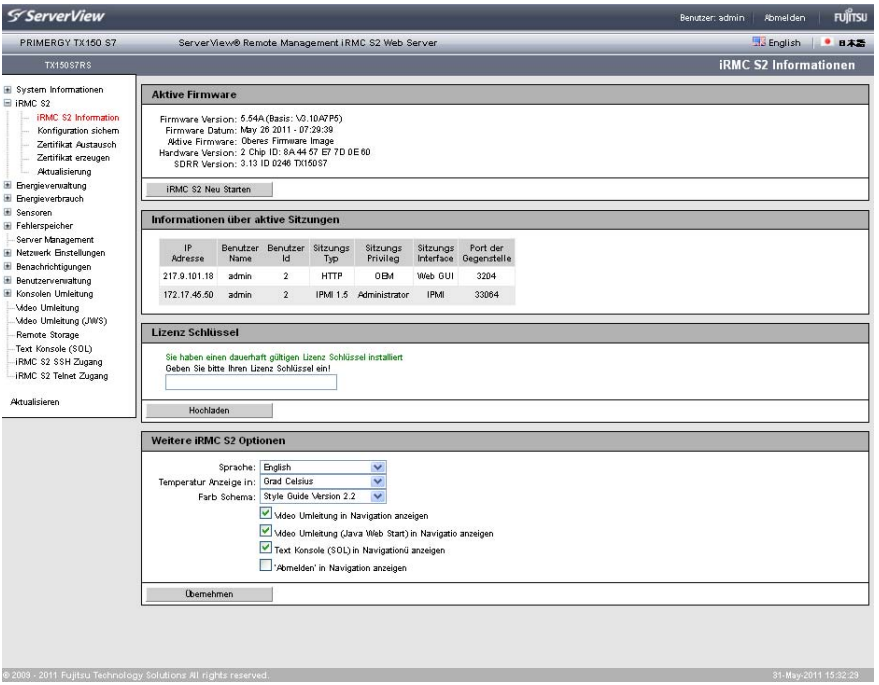


Bild 82: Seite iRMC S2/S3 Informationen

Aktive Firmware

Unter *Aktive Firmware* können Sie sich über Firmware- und SDRR-Version des iRMC S2/S3 informieren und den iRMC S2/S3 neu starten.

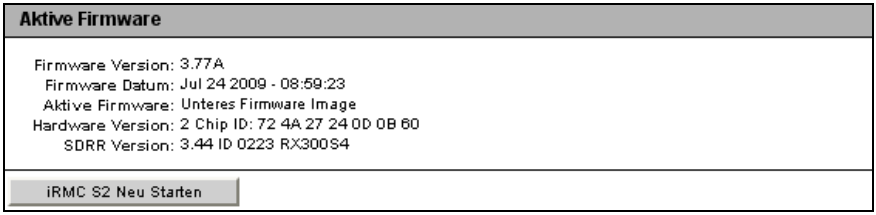

Aktive Firmware
Firmware Version: 3.77A
Firmware Datum: Jul 24 2009 - 08:59:23
Aktive Firmware: Unteres Firmware Image
Hardware Version: 2 Chip ID: 72 4A 27 24 0D 0B 60
SDRR Version: 3.44 ID 0223 RX300S4
iRMC S2 Neu Starten

Bild 83: Seite iRMC S2/S3 Informationen - Firmware Informationen und iRMC S2/S3 neu starten

iRMC S2/S3 neu starten

Startet den iRMC S2/S3 neu.

Die Schaltfläche iRMCS2/S3 neu starten ist während der BIOS POST-Phase des verwalteten Servers deaktiviert.

Informationen über aktive Sitzungen

In der Gruppe *Informationen über aktive Sitzungen* werden alle zurzeit aktiven iRMC S2/S3-Sitzungen angezeigt.

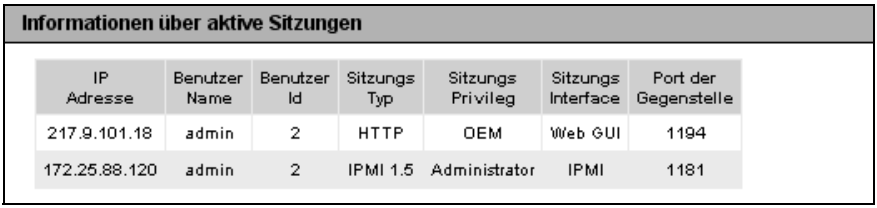


Bild 84: Seite iRMC S2/S3 Informationen - Informationen über aktive Sitzungen

Lizenz Schlüssel (License Key)

Mit der Gruppe *Lizenz Schlüssel* können Sie einen Lizenzschlüssel auf den iRMC S2/S3 laden.

Einen gültigen Lizenzschlüssel benötigen Sie, um die iRMC S2/S3-Funktionen *Grafische Konsolen Umleitung (Advanced Video Redirection)* (siehe Seite 312) und *Remote Storage* (siehe Seite 323) nutzen zu können.

Den Lizenzschlüssel können Sie käuflich erwerben.

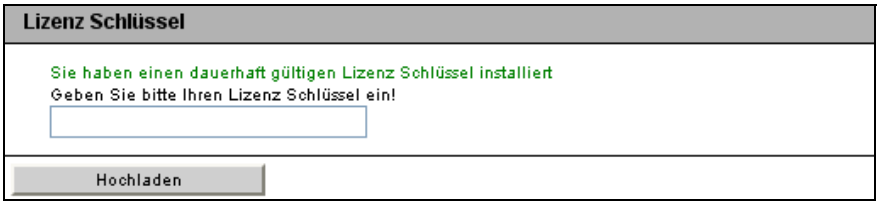

Lizenz Schlüssel
Sie haben einen dauerhaft gültigen Lizenz Schlüssel installiert
Geben Sie bitte Ihren Lizenz Schlüssel ein!
Hochladen

Bild 85: Seite iRMC S2/S3 Informationen - Lizenz Schlüssel

Hochladen

Wenn Sie auf diese Schaltfläche klicken, wird der im Eingabefeld spezifizierte Lizenzschlüssel auf den iRMC S2/S3 geladen.

Weitere iRMC S2/S3 Optionen

Mit der Gruppe *Weitere iRMC S2/S3 Optionen* können Sie Einstellungen für das Layout der iRMC S2/S3-Web-Oberfläche festlegen.

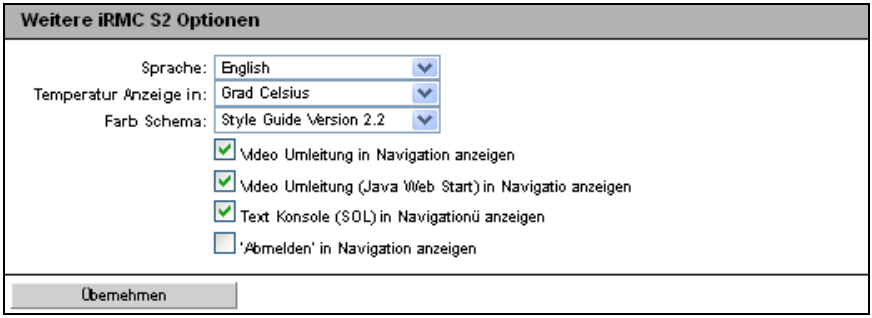


Bild 86: Seite iRMC S2/S3 Information - Weitere iRMC S2/S3 Optionen

Sprache

Legt die Landessprache (Deutsch/Englisch/Japanisch) fest, die beim nächsten Aufruf der iRMC S2/S3-Web-Oberfläche voreingestellt ist.

Temperatur Anzeige in

Legt die Einheit für die Anzeige von Temperaturwerten an der iRMC S2/S3-Web-Oberfläche fest (Grad Celsius / Grad Fahrenheit). Diese Einstellung gilt für die aktuelle Sitzung und ist beim nächsten Aufruf der iRMC S2/S3-Web-Oberfläche voreingestellt.

Farb Schema

Legt das Farbschema für die Anzeige der iRMC S2/S3-Web-Oberfläche fest. Diese Einstellung gilt die aktuelle Sitzung und ist beim nächsten Aufruf der iRMC S2/S3-Web-Oberfläche voreingestellt.

Video Umleitung in Navigation anzeigen

Fügt im Navigationsbereich zusätzlich den Link *Video Umleitung* ein, über den Sie die grafische Konsolen-Umleitung direkt starten können (siehe "Video Umleitung- AVR starten" auf Seite 319).

Video Umleitung(Java Web Start) in Navigation anzeigen

Fügt im Navigationsbereich zusätzlich den Link *Video Umleitung (JWS)* ein, über den Sie die grafische Konsolen-Umleitung (via Java Web Start) direkt starten können (siehe "Video Umleitung- AVR starten" auf Seite 319).

Text Console (SOL) in Navigationü anzeigen

Fügt im Navigationsbereich zusätzlich den Link *Text Konsole (SOL)* ein, über den Sie die Text Konsolen-Umleitung (via SOL) direkt starten können (siehe Abschnitt "Text Konsolen Umleitung (via Serial Over LAN) - Text-Konsolen-Umleitung starten" auf Seite 305).

'Abmelden' in Navigation anzeigen

Diese Option wird nur angeboten, wenn die Seite iRMC S2/S3 im Farbschema *StyleguideVersion 2.2* angezeigt wird.

Fügt den Link *Abmelden* zum Navigationsbereich hinzu, sodass Sie sich auch über den Navigationsbereich abmelden können.

7.6.2 iRMC S2/S3 Firmware Einstellungen abspeichern

Mithilfe der Seite *iRMC S2/S3 Firmware Einstellungen abspeichern* können Sie die aktuellen Firmware-Einstellungen sowie eine Reihe weiterer Einstellungen des iRMC S2/S3 in einer Datei abspeichern.

– Die unter *iRMC S2/S3 Firmware Einstellungen in ServerView® WinSCU XML Format abspeichern* ausgewählten Firmware-Einstellungen werden in der Datei *iRMC_S2_settings.pre* gesichert. Im WinSCU (siehe Seite 360) können Sie über die Schaltfläche *Import...* die Firmware-Settings wieder auf den iRMC S2/S3 laden.

– Die unter *iRMC S2/S3 Firmware Einstellungen in binär Format (BMCCLONE.exe) abspeichern* ausgewählten Firmware-Einstellungen werden in der Datei *iRMC_S2/S3_settings.bin* gesichert. Mithilfe der Gruppe *iRMC S2/S3 Firmware Einstellungen in ServerView® WinSCU XML Format importieren* können Sie die Firmware-Einstellungen wieder auf den iRMC S2/S3 laden.

ACHTUNG!

Sichern Sie die Einstellung grundsätzlich mithilfe der Variante *iRMC S2/S3 Firmware Einstellungen in ServerView® WinSCU XML Format abspeichern*.

Die Variante *iRMC S2/S3 Firmware Einstellungen in binär Format (BMCCLONE.exe) abspeichern* sollte nur bei Austausch der Systembaugruppe des verwalteten Servers verwendet werden.

Zum Abspeichern von Benutzereinstellungen (Option *Benutzer Einstellungen*) ist die *Benutzer konfigurieren erlaubt*-Berechtigung erforderlich, in den anderen Fällen genügt die Berechtigung *iRMC S2/S3 Einstellungen konfigurieren*.

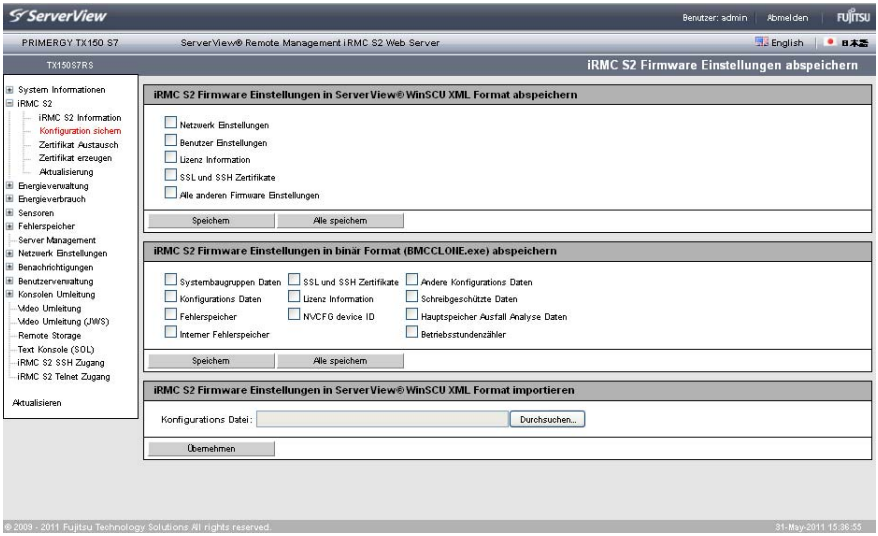


Bild 87: Seite iRMC S2/S3 Firmware Einstellungen abspeichern

iRMC S2/S3 Firmware Einstellungen in ServerView® WinSCU XML Format abspeichern

Speichern

Mit *Speichern* sichern Sie die gewählten Einstellungen.

Alle speichern

Mit *Alle speichern* sichern Sie alle Einstellungen.

iRMC S2/S3 Firmware Einstellungen in ServerView® WinSCU XML Format importieren

Konfigurations Datei

Konfigurationsdatei (Voreinstellung: *iRMC_S2/S3_settings.bin*) im ServerView® WinSCU XML-Format aus der Sie iRMC S2/S3-Firmware-Einstellungen auf den iRMC S2/S3 laden wollen.

Durchsuchen ...

Öffnet einen Datei-Browser, mit dem Sie zu der Konfigurationsdatei navigieren können.

7.6.3 Zertifikat Austausch - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden

Mit der Seite *Zertifikat Austausch* können Sie ein von einer Zertifizierungsstelle (Certificate Authority, CA) signiertes X.509 DSA/RSA-Zertifikat (SSL) und/oder Ihren privaten DSA/RSA-Schlüssel (SSH) auf den iRMC S2/S3 laden.

Der iRMC S2/S3 wird mit einem vordefinierten Server-Zertifikat (Standard-Zertifikat) ausgeliefert. Wenn Sie auf den iRMC S2/S3 über SSL/SSH-gesicherte Verbindungen zugreifen möchten, wird empfohlen, das Standard-Zertifikat möglichst bald durch ein Zertifikat zu ersetzen, das von einer Zertifizierungsstelle signiert ist.

Eingabeformat von X.509 DSA/RSA-Zertifikat und privatem DSA/RSA-Schlüssel:

X.509 DSA/RSA-Zertifikat und privater RSA/DSA-Schlüssel müssen jeweils in PEM-Codierung (ASCII/Base64) vorliegen.

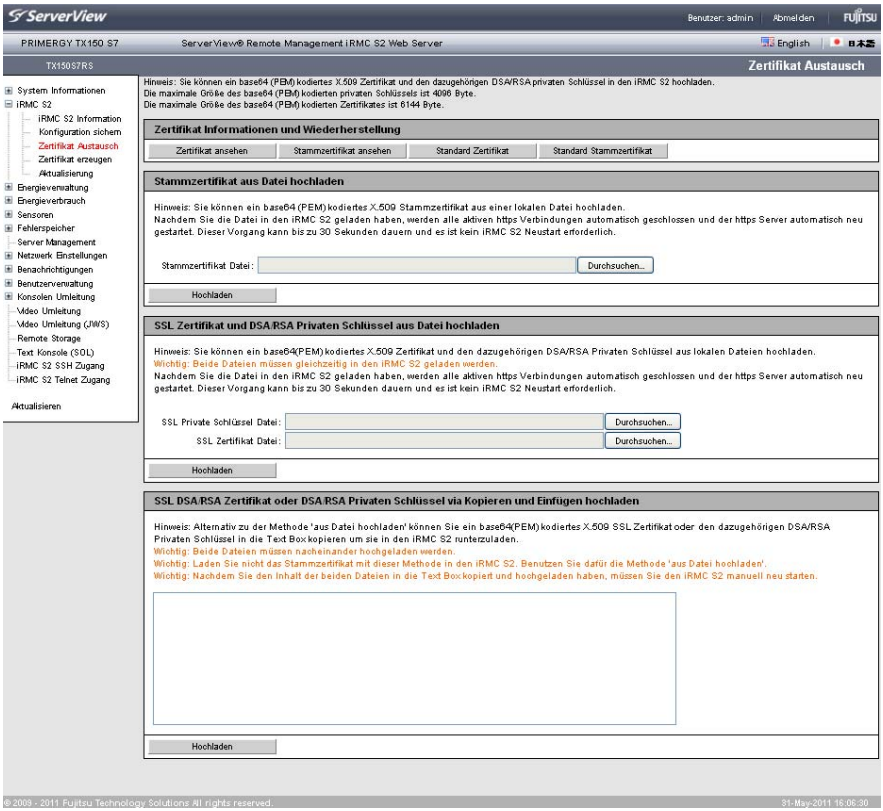


Bild 88: Seite Zertifikat Austausch

ktuell gültiges DSA/RSA-Zertifikat / Stammzertifikat anzeigen

- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Zertifikat ansehen*, um sich das aktuell gültige SSH/SSL-Zertifikat anzeigen zu lassen.
- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Stammzertifikat ansehen*, um sich das aktuell gültige Stammzertifikat (CA Certifikate) anzeigen zu lassen.

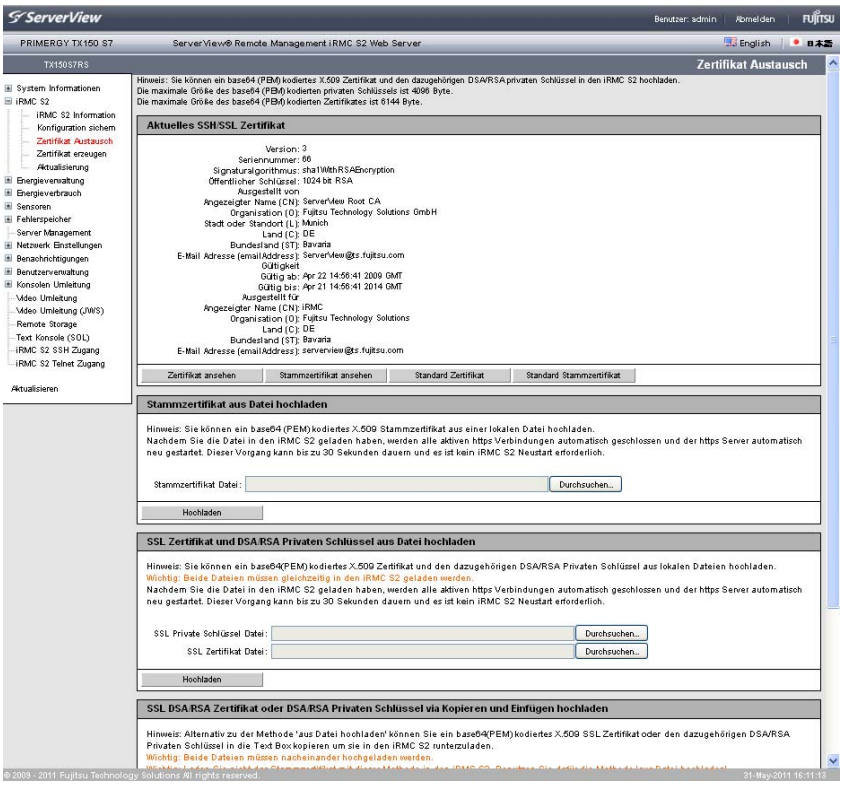


Bild 89: Seite Zertifikat Austausch - Anzeige des aktuell gültigen SSH/SSL-Zertifikats

Standard-Zertifikat / Standard-Stammzertifikat wiedereinsetzen

- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Standard Zertifikat*, um nach einem Bestätigungsdialog das Standard-Zertifikat wiedereinzusetzen, das mit der Firmware ausgeliefert wurde.
- Klicken Sie in der Gruppe Zertifikat Informationen und Wiederherstellung auf die Schaltfläche *Standard Stammzertifikat*, um nach einem Bestätigungsdialog das Standard-Stammzertifikat wiedereinzusetzen, das mit der Firmware ausgeliefert wurde.

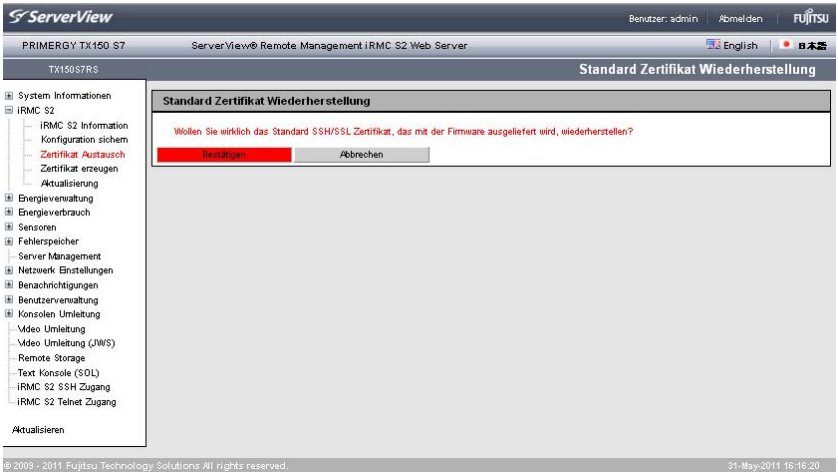


Bild 90: Seite Zertifikat Austausch - Standard Stammzertifikat wiedereinsetzen

Stammzertifikat aus einer lokalen Datei hochladen

Um ein Stammzertifikat aus einer lokalen Datei auf den iRMC S2/S3 zu laden, verwenden Sie die Gruppe *Stammzertifikat aus Datei hochladen*.

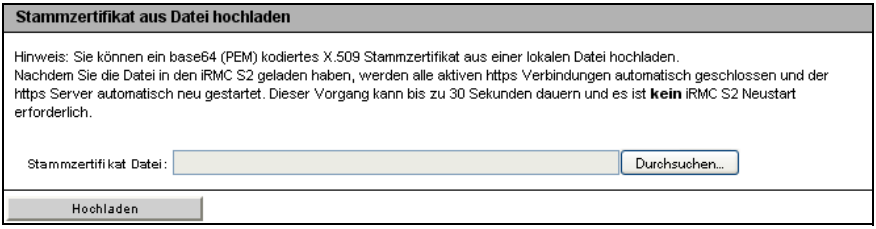


Bild 91: Stammzertifikat aus einer lokalen Datei hochladen

Gehen sie wie folgt vor:

- Speichern Sie das Stammzertifikat in einer lokalen Datei an Ihrem Remote-Arbeitsplatz.
- Spezifizieren Sie die Datei unter *Stammzertifikat Datei*, indem Sie auf die zugehörige Schaltfläche *Durchsuchen...* klicken und zur Datei navigieren, die das Stammzertifikat enthält.
- Klicken Sie auf die Schaltfläche *Hochladen,* um das Stammzertifikat auf den iRMC S2/S3 zu laden.

  Beim Hochladen des Stammzertifikats werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Dieser Vorgang kann bis zu 30 Sekunden dauern. Ein expliziter Neustart des iRMC S2/S3 ist **nicht** erforderlich.
- Klicken Sie auf die Schaltfläche *Stammzertifikat ansehen*, um sich vom erfolgreichen Hochladen des Stammzertifikats zu überzeugen.

SSL-Zertifikat und privaten DSA/RSA-Schlüssel aus lokalen Dateien hochladen

Hierfür verwenden Sie die Gruppe *SSL Zertifikat und DSA/RSA Privaten Schlüssel aus Datei hochladen*.

Privater Schlüssel und Zertifikat müssen gleichzeitig auf den iRMC S2/S3 geladen werden.

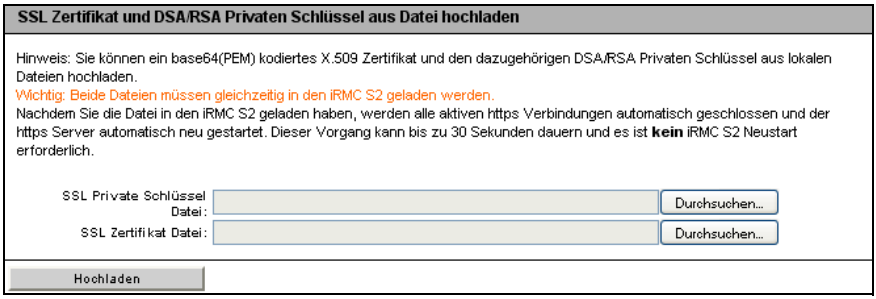


Bild 92: SSL-Zertifikat und privaten DSA/RSA-Schlüssel aus lokalen Dateien hochladen

Gehen Sie wie folgt vor:

- Speichern Sie den privaten DSA/RSA-Schlüssel und das SSL-Zertifikat jeweils in einer lokalen Datei an Ihrem Remote-Arbeitsplatz.
- Spezifizieren Sie unter *SSL Private Schlüssel Datei* und *SSL Zertifikat Datei* die Dateien für den privaten Schlüssel und das Zertifikat, indem Sie jeweils auf die zughörige Schaltfläche *Durchsuchen* klicken und zur Datei navigieren, die den privaten Schlüssel bzw. das Zertifikat enthält.
- Klicken Sie auf die Schaltfläche *Hochladen,* um das Zertifikat und den privaten Schlüssel auf den iRMC S2/S3 zu laden.

  Beim Hochladen von Zertifikat und privatem Schlüssel werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Dieser Vorgang kann bis zu 30 Sekunden dauern. Ein expliziter Neustart des iRMC S2/S3 ist **nicht** erforderlich.
- Klicken Sie auf die Schaltfläche *Zertifikat ansehen*, um sich vom erfolgreichen Hochladen des Zertifikats zu überzeugen.

DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Hierfür verwenden Sie die Gruppe *SSL DSA/RSA Zertifikat oder DSA/RSA Privaten Schlüssel via Kopieren und Einfügen hochladen*.

Verwenden Sie dieses Verfahren **nicht**, um ein Stammzertifikat auf den iRMC S2/S3 zu laden! Laden Sie ein Stammzertifikat immer via Datei (siehe Seite 182).

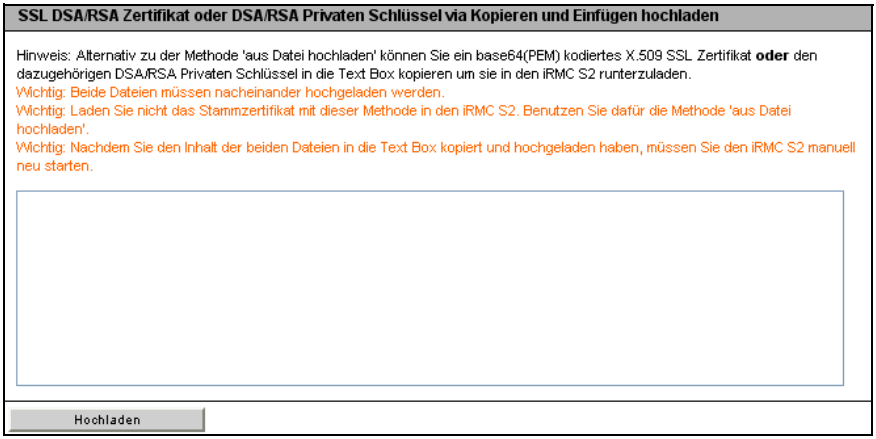


Bild 93: DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Gehen Sie wie folgt vor:

- Kopieren Sie das X.509 DSA-Zertifikat **oder** den privaten DSA-Schlüssel in den Eingabereich.

  Die gleichzeitige Eingabe von Zertifikat und Schlüssel für denselben Ladevorgang ist nicht zulässig.

- Klicken Sie auf die Schaltfläche *Hochladen,* um das Zertifikat oder den privaten Schlüssel auf den iRMC S2/S3 zu laden.

- Führen Sie mithilfe des Remote Manager einen Neustart (Reset) des iRMC S2/S3 durch (siehe Abschnitt "Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S2" auf Seite 350).

  Dies ist erforderlich, damit ein auf den iRMC S2/S3 geladenes Zertifikat oder privater Schlüssel gültig wird.

- Klicken Sie auf die Schaltfläche *Zeretifikat ansehen*, um sich vom erfolgreichen Hochladen des Zertifikats zu überzeugen.

7.6.4 Selbstsigniertes RSA Zertifikat erzeugen

Mit der Seite *Selbstsigniertes RSA Zertifikat erzeugen* können Sie ein selbstsigniertes RSA-Zertifikat erstellen.

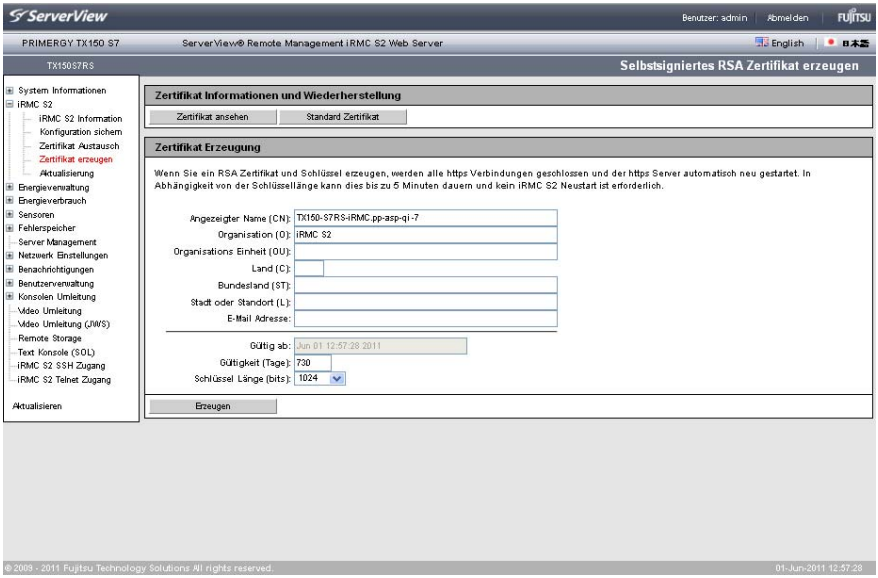


Bild 94: Seite Selbstsigniertes RSA Zertifikat erzeugen

Zertifikat Informationen und Wiederherstellung

Mit der Gruppe *Zertifikat Informationen und Wiederherstellung* können Sie sich das aktuell gültige DSA/RSA-Zertifikat ansehen und/oder das Standard-RSA/DSA-Zertifikat wiedereinsetzen.

Zertifikat ansehen

Mithilfe dieser Schaltfläche können Sie sich das aktuell gültige DSA/RSA-Zertifikat anzeigen lassen.

Standard Zertifikat

Mithilfe dieser Schaltfläche können Sie über einen Bestätigungsdialog das Standard-Zertifikat wiedereinsetzen, das mit der Firmware ausgeliefert wurde.

Zertifikat Erzeugung

Um ein selbstsigniertes RSA-Zertifikat zu erzeugen, gehen Sie wie folgt vor:

- Tragen Sie unter *Zertifikat Erzeugung* die erforderlichen Angaben ein.
- Klicken Sie auf die Schaltfläche *Erzeugen*, um das Zertifikat zu erzeugen.

> **i** Beim Generieren des neuen Zertifikats werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Je nach Schlüssellänge kann bis zu 5 Minuten dauern. Ein expliziter Neustart des iRMC S2/S3 ist **nicht** erforderlich.

7.6.5 iRMC S2/S3 Firmware Aktualisierung

Mit der Seite *iRMC S2/S3 Firmware Aktualisierung* können Sie die Firmware des iRMC S2/S3 online aktualisieren. Hierfür stellen Sie das aktuelle Firmware-Image wahlweise lokal am Remote-Arbeitplatz oder auf einem TFTP-Server bereit.

Außerdem erhalten Sie Informationen zur iRMC S2/S3-Firmware und können den Firmware-Selektor setzten.

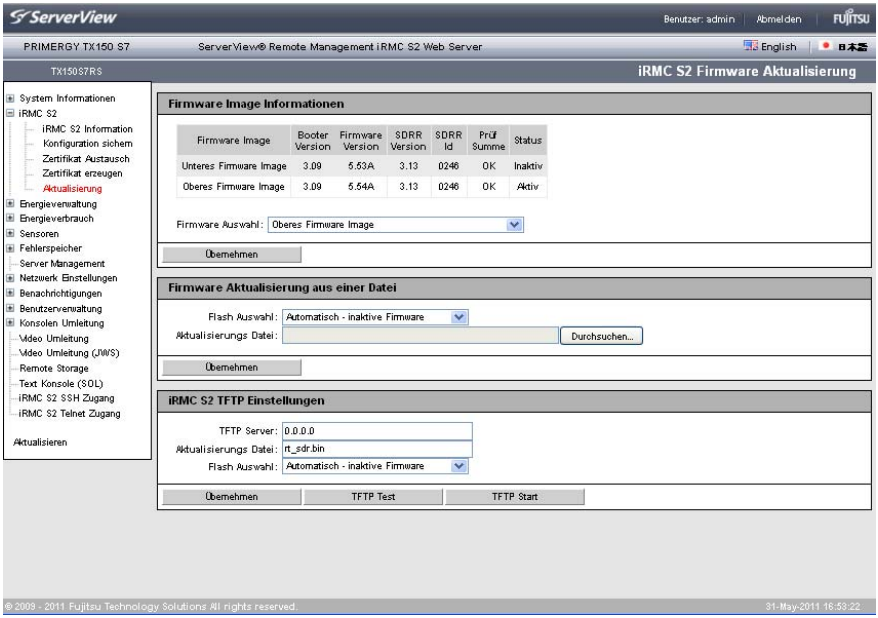


Bild 95: Seite iRMC S2/S3 Firmware Aktualisierung

Firmware Image Informationen

Unter *Firmware Image Information* können Sie Informationen zu Firmware- und SDRR-Version des iRMC S2/S3 einsehen sowie den Firmware-Selektor setzen.

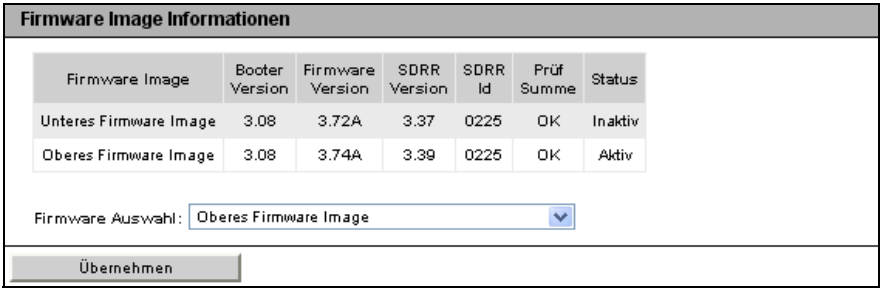


Bild 96: Seite iRMC S2/S3 Firmware Aktualisierung - Firmware Informationen

Firmware Auswahl

Mithilfe der Firmware-Auswahl (Firmware-Selektor) legen Sie fest, welches Firmware-Image nach dem nächsten Neustart des iRMC S2/S3 aktiv ist.

Folgende Möglichkeiten stehen zur Auswahl:

– *Automatisch - Firmware mit der höchsten Version*

  Es wird automatisch die Firmware mit dem aktuellsten Versionsstand ausgewählt.

– *Unteres Firmware Image*

  Es wird das untere Firmware-Image ausgewählt.

– *Oberes Firmware Image*

  Es wird das obere Firmware-Image ausgewählt.

– *Firmware mit der ältesten Firmware version*

  Es wird die Firmware mit dem ältesten Versionsstand ausgewählt.

– *Zuletzt programmierte Firmware*

  Es wird die zuletzt programmierte Firmware, also die Firmware mit dem aktuellsten Versionsstand ausgewählt.

– *Zuerst programmierte Firmware*

  Es wird die zuerst programmierte Firmware, also die Firmware mit dem ältesten Versionsstand ausgewählt.

Übernehmen

Mit *Übernehmen* setzen Sie den Firmware-Selektor auf die unter *Firmware Auswahl* gewählte Einstellung.

Firmware Aktualisierung aus einer Datei

Mit der Seite *Firmware Aktualisierung aus Datei* können Sie die Firmware des iRMC S2/S3 online aktualisieren. Hierfür stellen Sie das aktuelle Firmware-Image in einer Datei auf dem Remote-Arbeitsplatz bereit.

Das zu Ihrem PRIMERGY Server passenden Firmware-Image finden Sie auf der ServerView Suite DVD 1 bzw. zum Herunterladen unter *http://support.ts.fujitsu.com/com/support/downloads.html*.

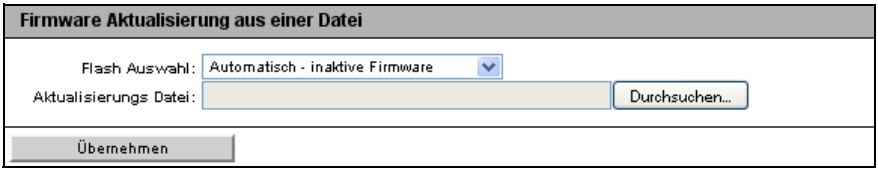


Bild 97: Seite iRMC S2/S3 Firmware Aktualisierung - Aktualisierung aus Datei

*Flash Auswah*l

Hier geben Sie an, welche Firmware des iRMC S2/S3 aktualisiert werden soll.

Folgende Möglichkeiten stehen zur Auswahl:

– *Automatisch - inaktive Firmware*

  Es wird automatisch die inaktive Firmware aktualisiert.

– *Unteres Firmware Image*

  Es wird das untere Firmware-Image (Firmware-Image 1) aktualisiert.

– *Oberes Firmware Image*

  Es wird das obere Firmware-Image (Firmware-Image 2) aktualisiert.

Aktualisierungs Datei

Datei, die das Firmware-Image enthält.

Mithilfe der nachfolgend genannten Dateien können Sie pro Aktualisierungslauf je einen Bestandteil der iRMC S2/S3-Firmware (Runtime-Firmware und SDR-Datensatz) aktualisieren.

Für einige PRIMERGY Server / Blade-Server steht außerdem die Datei *rt_sdt_<D-Nummer>_4_08g_00.bin* zur Verfügung, mit der Sie alle Bestandteile der iRMC S2/S3-Firmware in einem Arbeitsgang aktualisieren können.

dcod<FW-Version>.bin

Aktualisierung der Runtime-Firmware.

<SDR-Version>.SDR

Aktualisierung des SDR-Datensatzes.

Durchsuchen...

Öffnet einen Datei-Browser, mit dem Sie zur Aktualisierungsdatei navigieren können.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren und die Aktualisierung der iRMC S2/S3 Firmware zu starten.

iRMC S2/S3 TFTP Einstellungen

Mit der Seite *iRMC S2/S3 TFTP Firmware Einstellungen* können Sie die Firmware des iRMC S2/S3 online aktualisieren. Hierfür stellen Sie das aktuelle Firmware-Image auf einem TFTP-Server bereit.

Das zu Ihrem PRIMERGY Server passenden Firmware-Image finden Sie auf der ServerView Suite DVD 1 bzw. zum Herunterladen unter *http://support.ts.fujitsu.com/com/support/downloads.html*.

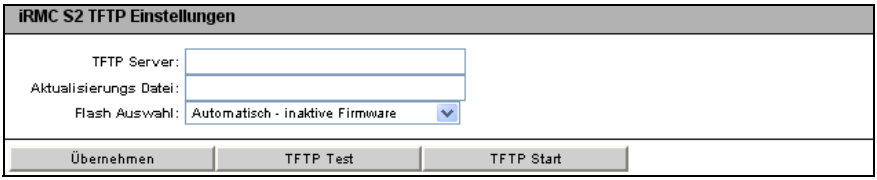


Bild 98: Seite iRMC S2/S3 Firmware Aktualisierung - iRMC S2/S3 Firmware Einstellungen

TFTP Server
: IP-Adresse oder DNS Name des TFTP-Servers, auf dem das Firmware-Image abgelegt ist.

Aktualisierungs Datei
: Datei, die das Firmware-Image enthält.

> **i** Mithilfe der nachfolgend genannten Dateien können Sie pro *TFTP Start* je einen Bestandteil der iRMC S2/S3-Firmware (Runtime-Firmware und SDR-Datensatz) aktualisieren.
>
> Für einige PRIMERGY Server / Blade-Server steht außerdem die Datei *rt_sdt_<D-Nummer>_4_08g_00.bin* zur Verfügung, mit der Sie via TFTP-Server alle Bestandteile der iRMC S2/S3-Firmware in einem Arbeitsgang aktualisieren können.

dcod<FW-Version>.bin
: Aktualisierung der Runtime-Firmware.

<SDR-Version>.SDR
: Aktualisierung des SDR-Datensatzes.

Flash Auswahl

Hier geben Sie an, welche Firmware des iRMC S2/S3 aktualisiert werden soll.

Folgende Möglichkeiten stehen zur Auswahl:

– *Automatisch - inaktive Firmware*

  Es wird automatisch die inaktive Firmware aktualisiert.

– *Unteres Firmware Image*

  Es wird das untere Firmware-Image (Firmware-Image 1)aktualisiert.

– *Oberes Firmware Image*

  Es wird das obere Firmware-Image (Firmware-Image 2) aktualisiert.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Klicken Sie auf die Schaltfläche *TFTP Test*, um die Verbindung zum TFTP-Server zu testen.

► Klicken Sie auf die Schaltfläche *TFTP Start*, das Firmware-Image vom TFTP-Server herunterzuladen und die Aktualisierung der iRMC S2/S3-Firmware zu starten.

7.7 Energieverwaltung

Der Eintrag *Energieverwaltung* enthält die Verweise auf die Seiten für die Energieverwaltung Ihres PRIMERGY Servers:

– "Ein-/Ausschalten - Server ein-/ausschalten" auf Seite 194.

– "Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren" auf Seite 198.

– "Netzteil Information - Stromversorgung und IDPROM-Daten der FRU-Komponenten" auf Seite 205.

7.7.1 Ein-/Ausschalten - Server ein-/ausschalten

Über die Seite *Ein-/Ausschalten* können Sie den verwalteten Server ein- und ausschalten. Sie werden über die aktuelle Energieversorgung des Servers informiert und können außerdem das Verhalten des Servers beim nächsten Neustart konfigurieren.

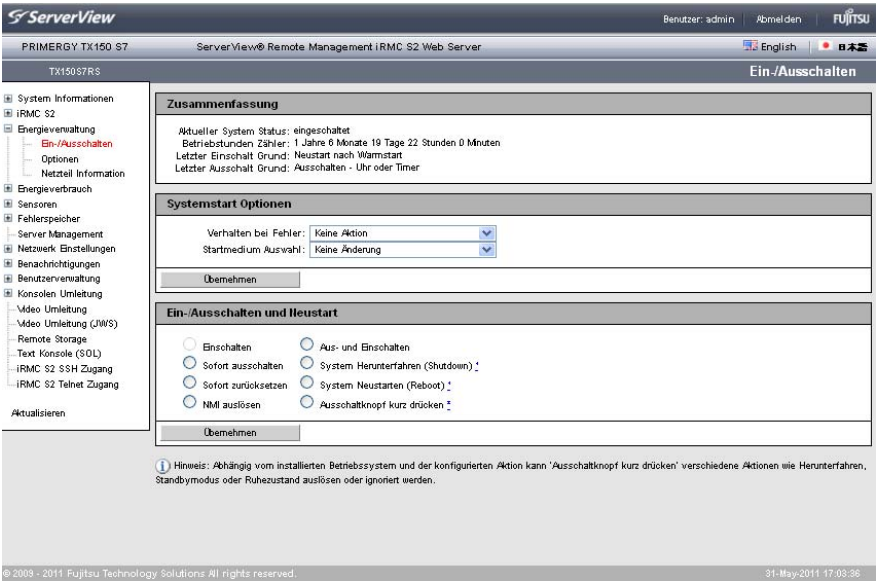


Bild 99: Seite Ein-/Ausschalten

Zusammenfassung

In der Gruppe *Zusammenfassung* werden Sie über die aktuelle Stromversorgung des Servers sowie über die Ursachen für das zuletzt durchgeführte An- und Abschalten informiert. Außerdem summiert ein Zähler die Monate, Tage und Minuten, die der Server bisher insgesamt eingeschaltet war.

Zusammenfassung
Aktueller System Status: eingeschaltet
Betriebstunden Zähler: 1 Jahre 4 Monate 15 Tage 8 Stunden 55 Minuten
Letzter Einschalt Grund: Neustart nach Warmstart
Letzter Ausschalt Grund: Ausschalten - Ausschalt Knopf
Bild 100: Seite Ein-/Ausschalten - Zusammenfassung

Systemstart Optionen

Mit der Gruppe *Systemstart Optionen* konfigurieren Sie das Verhalten des Systems beim **nächsten** Neustart des Servers. So können Sie festlegen, von welchem Medium das System gestartet werden soll, und ob das BIOS den Startvorgang unterbrechen soll, wenn während der POST-Phase Fehler auftreten.

Die hier eingestellten Optionen gelten nur für den nächsten Startvorgang. Danach ist wieder der voreingestellte Mechanismus wirksam.

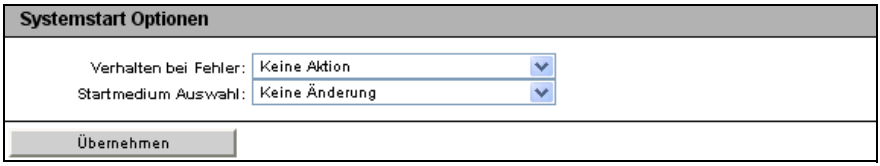


Bild 101: Seite Ein-/Ausschalten - Systemstart Optionen

- Wählen Sie unter *Verhalten bei Fehler* das gewünschte BIOS-Verhalten:

  Keine Aktion
  Startvorgang des Systems fortsetzen, wenn während der POST-Phase Fehler auftreten.

  Bei Fehler anhalten
  Startvorgang des Systems unterbrechen, wenn während der POST-Phase Fehler auftreten.

- Wählen Sie unter *Startmedium Auswahl* das Speichermedium, von dem das System gestartet werden soll.

  Folgende Alternativen stehen zur Auswahl:

  - *Keine Änderung*: Es wird erneut vom selben Speichermedium gestartet.
  - *PXE/iSCSI*: Es wird über das Netz von PXE / iSCSI gestartet.
  - *Festplatte*: Es von der Festplatte gestartet.
  - *CDROM/DVD*: Es wird von CD /DVD gestartet.
  - *Diskette*: Es wird von Diskette gestartet.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Ein-/Ausschalten und Neustart - Server ein-/ausschalten, neu starten

Mit der Gruppe *Ein-/Ausschalten und Neustart* können Sie den Server ein- und ausschalten oder einen Neustart durchführen.

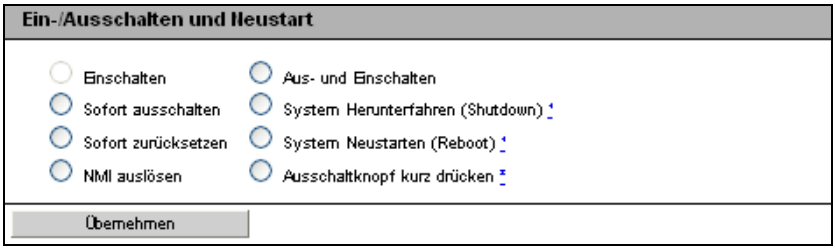


Bild 102: Seite Ein-/Ausschalten - Ein-/Ausschalten und Neustart (Server ist eingeschaltet)

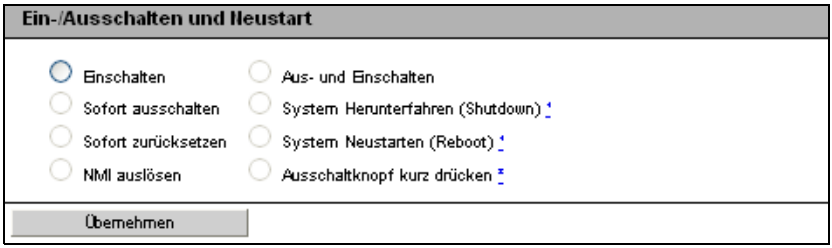


Bild 103: Seite Ein-/Ausschalten - Ein-/Ausschalten und Neustart (Server ist ausgeschaltet)

Einschalten
: Schaltet den Server ein.

Sofort ausschalten
: Schaltet den Server unabhängig vom Status des Betriebssystems aus.

Sofort zurücksetzen
: Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).

NMI auslösen
: Löst eine nicht-maskierbare Unterbrechung (non-maskable interrupt, NMI) aus. Ein NMI ist eine Prozessorunterbrechung, die nicht von Standard-Unterbrechungsmaskierung des Systems ignoriert werden kann.

Ausschaltknopf kurz drücken

Abhängig vom installierten Betriebssystem und der konfigurierten Aktion können Sie mit *Ausschaltknopf kurz drücken* unterschiedliche Aktionen auslösen wie Herunterfahren, Standby-Modus oder Ruhezustand auslösen.

Aus- und Einschalten

Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein. Diese Zeit können Sie im Eingabefeld *Aus-/ Einschalt Verzögerung* der Gruppe *ASR&R Einstellungen* (siehe Seite 240) konfigurieren.

System Herunterfahren (Shutdown)

System „sanft“ herunterfahren und ausschalten.
Diese Option ist nur verfügbar, wenn die ServerView-Agenten installiert und beim iRMC S2/S3 als „Connected“ gemeldet sind.

System Neustarten (Reboot)

System „sanft“ herunterfahren und anschließend neu starten.
Diese Option ist nur verfügbar, wenn die ServerView-Agenten installiert und beim iRMC S2/S3 als „Connected“ gemeldet sind.

► Klicken Sie auf die Schaltfläche *Übernehmen,* um die gewünschte Aktion zu starten.

7.7.2 Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren

Über die Seite *Energieverwaltungsoptionen* können Sie das Verhalten des Servers nach Stromausfall und die Ein-/Ausschaltzeiten des Server festlegen.

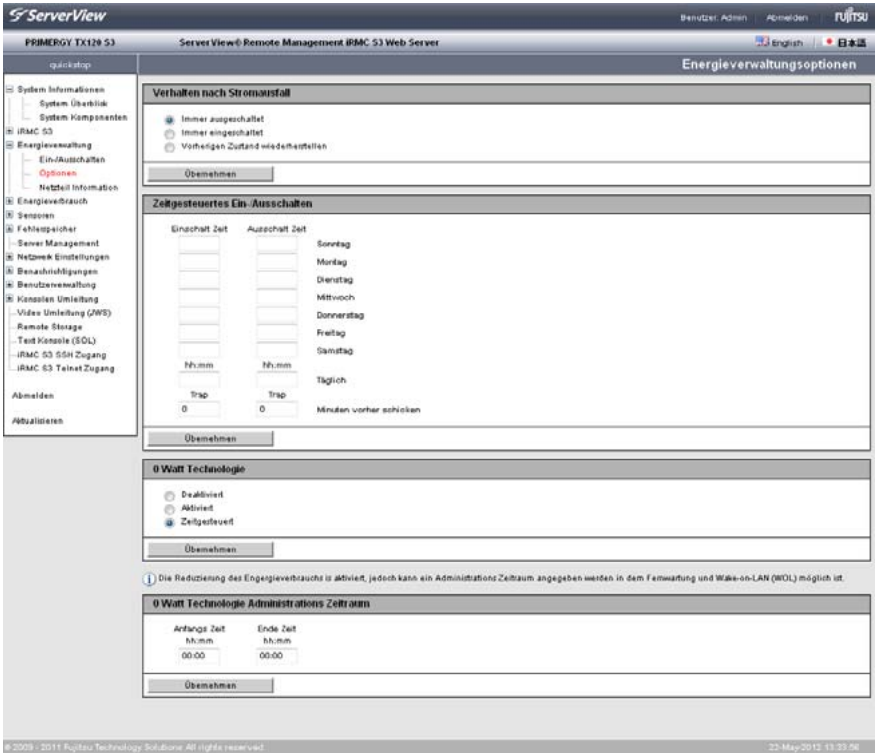


Bild 104: Seite Energieverwaltunsgoptionen

Verhalten nach Stromausfall

Mit der Gruppe *Verhalten nach Stromausfall* konfigurieren Sie die Energieverwaltung für den Server nach einem Stromausfall.

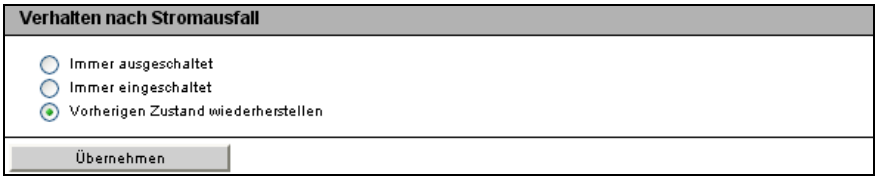


Bild 105: Seite Energieverwaltung Optionen - Verhalten nach Stromausfall

Immer ausgeschaltet
: Nach Stromausfall bleibt der Server immer ausgeschaltet.

Immer eingeschaltet
: Nach Stromausfall wird der Server jedesmal wieder eingeschaltet.

Vorherigen Zustand wiederherstellen
: Die Energieversorgung des Servers wird auf den Status der Energieversorgung vor dem Stromausfall gesetzt.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Die konfigurierte Aktion wird nach einem Stromausfall ausgeführt.

Zeitgesteuertes Ein-/Ausschalten

In den Eingabefeldern der Gruppe *Zeitgesteuertes Ein-/Ausschalten* spezifizieren Sie die Ein-/Ausschalt-Zeiten des Servers an den einzelnen Wochentagen oder - einheitlich für alle Wochentage - die täglichen Ein-/Ausschalt-Zeiten.

Die Angaben im Eingabefeld *Täglich* haben Vorrang!

Außerdem können Sie in den Feldern *Trap* festlegen, ob und gegebenenfalls wieviele Minuten vor einem geplanten Ein-/Ausschalten des verwalteten Servers der iRMC S2/S3 einen SNMP-Trap an die Management-Konsole senden soll. Wenn Sie den Wert „0“ angeben, werden keine Traps gesendet.

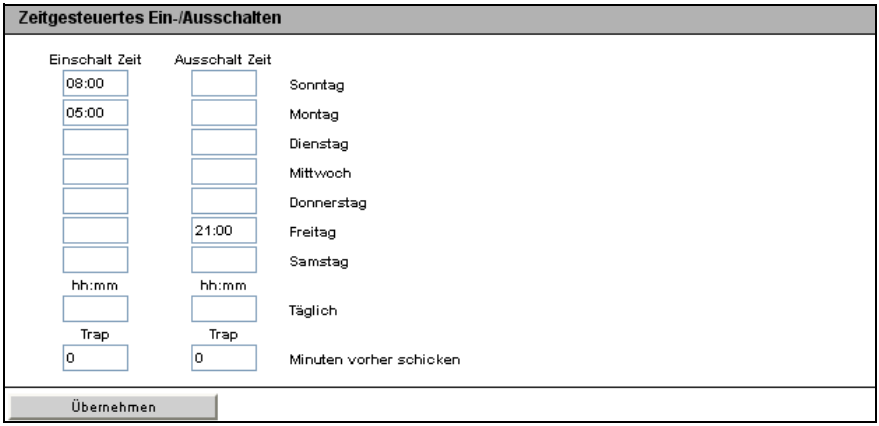


Bild 106: Seite Energieverwaltung Optionen - Zeitgesteuertes Ein-/Ausschalten

► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

0 Watt Technologie

Beachten Sie:

– Diese Funktion wird nur vom iRMC S3 unterstützt.

– Diese Funktion wird nicht für alle PRIMERGY Server unterstützt.

Die Funktionalität "0 Watt-Technologie"ermöglicht es Ihnen, den Standby-Stromverbrauch Ihres Servers auf 0 Watt zu reduzieren. Bei jedem Ausschalten des Servers wird der Standby-Stromverbrauch Ihres Servers auf 0 Watt reduziert (*0 Watt*-Modus)

Im *0 Watt*-Modus ist eine Remote-Verwaltung des Servers nicht mehr möglich. Der Server kann nur durch Drücken der Einschalttaste oder der Not-Einschalttaste der Stromversorgungseinheit (Power Supply Unit, PSU) eingeschaltet werden.

Über die Option *Zeitgesteuert* (siehe Seite 204) können Sie ein Zeitintervall festlegen, währenddessen die Stromversorgungseinheit aus dem *0 Watt*-Modus geweckt wird und somit auch Remote-Management und Wake-on-LAN (WOL) möglich sind.

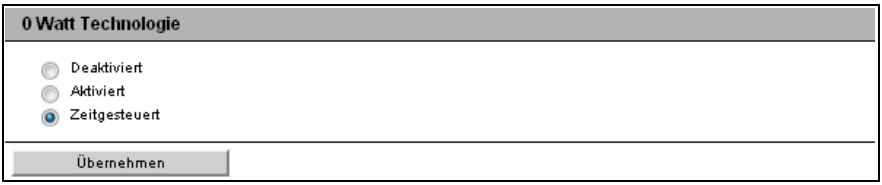


Bild 107: Seite Energieverwaltung, 0 Watt Technologie

Deaktiviert

Deaktiviert den *0 Watt*-Modus und verbleibt im / schaltet in den Standard-Modus für das Ein-/Ausschalten. Der Server kann jederzeit via Remote Management verwaltet werden.

Aktiviert

Aktiviert den *0 Watt*-Modus.

Auch wenn *Aktiviert* konfiguriert ist, ist *0 Watt*-Modus in folgenden Fällen blockiert:

- Aus- und Einschalten / Einschaltverzögerung

  Ein Aus- und Einschalten-Zyklus schaltet den Server aus, ohne den *0 Watt*-Modus zu aktivieren, d.h. während der Ein- und Ausschalt-Verzögerung innerhalb eines Zyklus wird der *0 Watt*-Modus wird nicht aktiviert:

  – Jede Einschalt-Aufforderung, die während der Verzögerungsphase eingeht, führt zum Einschalten des Servers im Anschluss an die Verzögerungsphase.

  – Falls während der Verzögerungsphase keine Einschalt-Aufforderung eingeht, aktiviert der iRMC S3 den *0 Watt*-Modus im Anschluss an die Verzögerungsphase.

- Temperaturbedingte (Wieder-)Einschalt-Verhinderung

  Falls im BIOS/UEFI Setup-Menü der *Temperature Monitoring*-Modus aktiviert wurde, wird der *0 Watt*-Modus nicht aktiviert.

- ASR&R

  Jede ASR&R-Aktion, die gerade dabei ist, den Wiederholungszähler herunterzuzählen, verhindert die Aktivierung des *0 Watt*-Modus. Dies trifft sogar dann zu, wenn der Server nach Erreichen von Wiederholungszähler=0 ausgeschaltet wurde.

- *Zeitgesteuertes Ein-/Ausschalten* (siehe "Zeitgesteuertes Ein-/Ausschalten" auf Seite 200)

  Solange Zeitgesteuertes Ein-/Ausschalten in der Seite *Power Options* aktiviert ist, kann der *0 Watt*-Modus nicht aktiviert werden.

  Der *0 Watt*-Modus kann auch nicht aktiviert werden, wenn der *Ein-/Ausschalten*-Timer deaktiviert wird, während der Server ausgeschaltet ist. In diesem Fall wird der *0 Watt*-Modus erst beim nächsten Ausschalten aktiviert. Somit wird ein zeitgesteuerter *Ein-/Ausschalten*-Timer die Aktivierung des *0 Watt*-Modus nicht verhindern.

- Fehler-LED (Global Error-LED)

  Sobald die Fehler-LED einen problematischen Systemzustand anzeigt, aktiviert der iRMC S3 den *0 Watt*-Modus nicht. Grund: Der iRMC S3 muss auch bei ausgeschaltetem System problematische Systemzustände melden können.

- Identifizierungs-LED

  Bei eingeschalteter Identifizierungs-LED aktiviert der iRMC S3 den *0 Watt*-Modus nicht.

- Advanced Video Redirection (AVR)

  Solange eine AVR-Sitzung aktiv ist, aktiviert der iRMC S3 den *0 Watt*-Modus nicht. Der iRMC S3 aktiviert den *0 Watt*-Modus, sobald alle AVR-Sitzungen beendet sind (d.h. die AVR ist nicht aktivist).

- Remote Storage Server (RSS), Telnet/SSH-Sitzungen

  Solange eine RSS-Sitzung oder eine SSH/Telnet-Sitzung aktiv ist, aktiviert der iRMC S3 den *0 Watt*-Modus nicht. Dies verhindert, dass die entsprechenden Remote-Verbindungen zum iRMC S3 verloren gehen.

- Fehlerhafte Stromversorgung

  Wenn ein Fehler in der Stromversorgung auftritt, während das Stromversorgungseinheit (Power Supply Unit, PSU) sich im *0 Watt*-Modus oder im zeitgesteuerten Modus befindet, kehrt die PSU zum Standby-Modus zurück. Je nach konfiguriertem Verhalten bei Stromausfall (siehe Seite 199) entscheidet der iRMC S3, ob der Server eingeschaltet wird. Wenn die Einstellung *Immer ausgeschaltet* konfiguriert ist, wird ein Fehler in der Stromversorgung niemals im *0 Watt*-Modus resultieren. Der im *0 Watt*-Modus kann eventuell nach dem nächsten Einschalten des Systems erreicht werden.

Scheduled

Aktiviert den *0 Watt*-Modus und zeigt die Gruppe *0 Watt Technologie Administrations Zeitraum* an. Mit der Gruppe *0 Watt Technologie Administrations Zeitraum* können Sie ein Zeitintervall festlegen, währenddessen die Stromversorgungseinheit (Power Supply Unit, PSU) aus dem *0 Watt*-Modus geweckt wird und und somit Remote-Management und Wake-on-LAN (WOL) möglich sind.

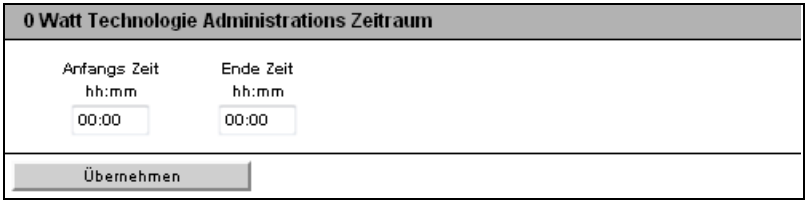


Bild 108: Seite Energieverwaltung, 0 Watt Technologie Administrations Zeitraum

Anfangs Zeit

Definiert den Anfang (*hh:mm*) des Zeitintervalls.

Ende Zeit

Definiert das Ende (*hh:mm*) des Zeitintervalls.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

7.7.3 Netzteil Information - Stromversorgung und IDPROM-Daten der FRU-Komponenten

Auf Seite *Netzteil Information* können Sie sich über die Spezifikationen für die Stromversorgung sowie über die IDPROM-Daten der FRUs des Servers informieren.

In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice)-Funktionalität unterstützt wird.

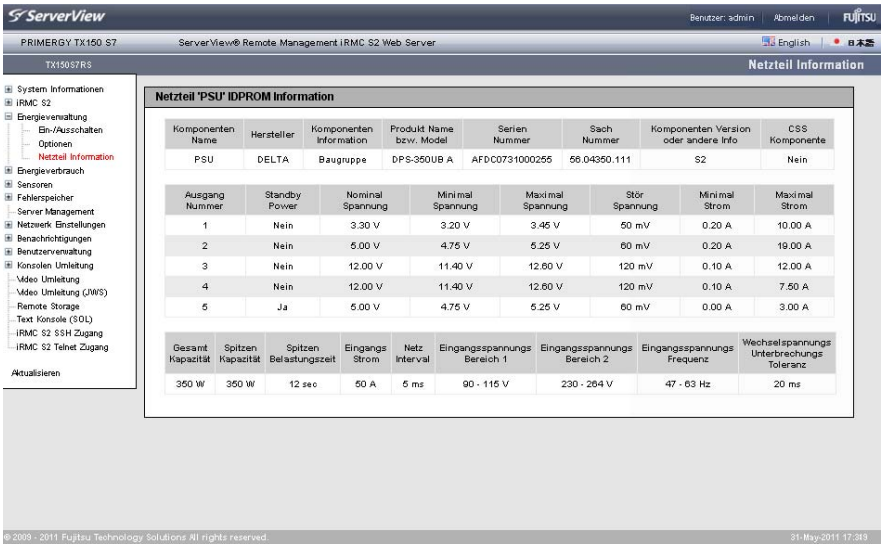


Bild 109: Seite Netzteil Information

7.8 Energieverbrauch - Energieverbrauch des Servers steuern

Der Eintrag *Energieverbrauch* enthält die Verweise auf die Seiten zur Steuerung und Kontrolle des Energieverbrauchs des verwalteten Servers:

– "Konfiguration der Energieverbrauchssteuerung - Energieverbrauch des Servers konfigurieren" auf Seite 207

– "Aktueller System Energieverbrauch - aktuellen Energieverbrauch anzeigen" auf Seite 213 (Wird nicht von allen Servern mit iRMC S2/S3 unterstützt.)

– "Energieverbrauch Verlauf - zeitlichen Verlauf des Energieverbrauchs anzeigen" auf Seite 214 (Wird nicht von allen Servern mit iRMC S2/S3 unterstützt.)

7.8.1 Konfiguration der Energieverbrauchssteuerung - Energieverbrauch des Servers konfigurieren

Auf der Seite *Konfiguration der Energieverbrauchssteuerung* können Sie den Modus spezifizieren, nach dem der iRMC S2/S3 den Energieverbrauch Ihres PRIMERGY Servers steuert.

Bild 110: Seite Konfiguration der Energieverbrauchssteuerung (nicht zeitgesteuert)

Voraussetzung:

Um die Energieverbrauchssteuerung konfigurieren können, müssen folgende Voraussetzungen erfüllt sein:

- Der verwaltete PRIMERGY Server unterstützt dieses Feature.
- Im Menü *Advanced* des BIOS Setup muss *Enhanced Speed Step* oder *Processor Power Management* aktiviert sein.

Wenn Sie unter *Optionen des Energieverbrauchs* den Verbrauchsmodus „zeitgesteuert“ aktivieren, wird zusätzlich die Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* angezeigt (siehe Seite 209).

Wenn Sie unter *Optionen des Energieverbrauchs* oder innerhalb der *Konfiguration des zeitgesteuerten Energieverbrauchs* den Verbrauchsmodus „Begrenzung des Energieverbrauchs“ aktivieren, wird zusätzlich die Gruppe *Begrenzung des Energieverbrauchs* angezeigt (siehe Seite 209).

Optionen des Energieverbrauchs

In der Gruppe *Optionen des Energieverbrauchs* können Sie den Modus für die Verbrauchssteuerung wählen und festlegen, ob der zeitliche Verlauf des Energieverbrauchs aufgezeichnet werden soll

Energieverbrauch Modus

Modus für die Steuerung des Energieverbrauchs des verwalteten Servers:

- *Verbrauchs Steuerung deaktiviert*:

  Der iRMC S2/S3 überlässt die Steuerung des Energieverbrauchs dem Betriebssystem.

- *Beste Performance*:

  Der iRMC S2/S3 steuert den Server im Hinblick auf beste Performance. Der Energieverbrauch kann in diesem Fall ansteigen.

- *Begrenzung des Geräuschpegels*: (nur iRMC S3)

  Der iRMC S3 steuert den Server mit dem Ziel, einen möglichst niedrigen Geräuschpegel zu erzielen. Diese Funktionalität wird nicht für alle PRIMERGY Server unterstützt und ist nur für bestimmte Konfigurationen verfügbar.

- *Minimaler Energieverbrauch*:

  Der iRMC S2/S3 steuert den Server im Hinblick auf möglichst geringen Energieverbrauch. In diesem Fall ist die Performance nicht immer optimal.

- *Begrenzung des Energieverbrauchs*:

  Die Gruppe *Begrenzung des Energieverbrauchs* angezeigt (siehe "Optionen der Energieverbrauchsbegrenzung" auf Seite 211).

- *Zeitgesteuert*:

  Wenn Sie *Zeitgesteuert* aktivieren, wird in der Seite *Konfiguration des Energieverbrauchs* zusätzlich die Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* angezeigt (siehe "Konfiguration des zeitgesteuerten Energieverbrauchs" auf Seite 209).

Energieverbrauch Anzeige Einheiten

Einheit der elektrischen Leistung für die Anzeige des Energieverbrauchs:

- *Watt*
- *BTU/h* (British Thermal Unit/hour, 1 BTU/h entspricht 0,293 Watt).

Verbrauchsaufzeichnung aktiviert

Wenn Sie diese Option aktivieren, wird der zeitliche Verlauf des Energieverbrauchs aufgezeichnet.

Die Verbrauchsaufzeichnung (Power Monitoring) ist ab Firmware Version 3.32 standardmäßig aktiviert.

Diese Einstellung ist nur wirksam bei PRIMERGY Servern, die Verbrauchsaufzeichnung unterstützen.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Konfiguration des zeitgesteuerten Energieverbrauchs

Mit der Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* können Sie detailliert die Zeitpläne und Modi (Betriebssystem-gesteuert, beste Performance, minimaler Energieverbrauch) festlegen, nach denen der iRMC S2/S3 den Energieverbrauch am verwalteten Server steuert.

Die Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* wird nur dann angezeigt, wenn Sie in der Gruppe *Optionen des Energieverbrauchs* den Verbrauchsmodus *zeitgesteuert* aktiviert haben.

Die Konfiguration des zeitgesteuerten Energieverbrauchs setzt voraus, dass im BIOS Setup die Einstellung *Enhanced Speed Step* aktiviert wurde. Andernfalls wird ein entsprechender Hinweis angezeigt.

Wenn dieser Hinweis trotz aktiviertem „Enhanced Speed Step“ angezeigt wird, kann dies folgende Ursachen haben:

- Die CPU (z.B. Low Power CPU) des Servers unterstützt nicht den zeitgesteuerten Energieverbrauch.
- Das System befindet sich in der BIOS POST-Phase.

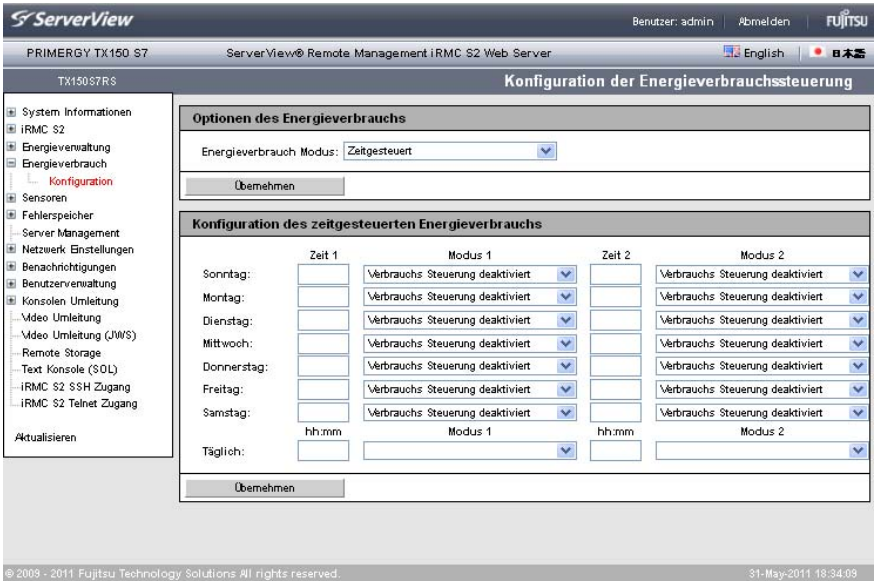


Bild 111: Seite Konfiguration der Energieverbrauchssteuerung (zeitgesteuert)

Zeit 1

Zeitpunkt [hh:ss], zu dem der iRMC S2/S3 am zugehörigen Wochentag mit der Verbrauchssteuerung gemäß *Modus 1* startet.

Zeit 2

Zeitpunkt [hh:ss], zu dem der iRMC S2/S3 am zugehörigen Wochentag mit der Verbrauchssteuerung gemäß *Modus 2* startet.

Modus 1

Verbrauchsmodus, gemäß dem der iRMC S2/S3 die Verbrauchssteuerung am zugehörigen Wochentag ab dem Zeitpunkt *Zeit 1* durchführt.

Modus 2

Verbrauchsmodus, gemäß dem der iRMC S2/S3 die Verbrauchssteuerung am zugehörigen Wochentag ab dem Zeitpunkt *Zeit 2* durchführt.

Wählen Sie *Zeit 1* < *Zeit 2*, da andernfalls der unter *Modus 2* festgelegte Verbrauchsmodus erst zu *Zeit 2* am entsprechenden Tag der darauffolgenden Woche aktiviert wird.

Die Angaben bei *Täglich* haben Vorrang.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Den zeitgesteuerten Energieverbrauch können Sie auch über den Server Configuration Manager konfigurieren (siehe Kapitel "iRMC S2/S3 via Server Configuration Manager konfigurieren" auf Seite 359).

Optionen der Energieverbrauchsbegrenzung

Die Gruppe *Optionen der Energieverbrauchsbegrenzung* wird in folgenden Fällen angezeigt:

– In der Gruppe *Optionen des Energieverbrauchs* ist der Verbrauchsmodus *Begrenzung des Energieverbrauchs* ausgewählt und aktiviert.

– In der Gruppe *Optionen des Energieverbrauchs* ist der Verbrauchsmodus *Zeitgesteuert* aktiviert, und in der Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* ist mindestens einmal der Verbrauchsmodus *Begrenzung des Energieverbrauchs* aktiviert.

  Die Verbrauchsbegrenzung gilt dann für alle Zeitspannen, für die in der Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* dieser Verbrauchsmodus aktiviert ist.

Bild 112: Seite Konfiguration der Energieverbrauchssteuerung (zeitgesteuert)

Verbrauch begrenzen

Maximale Leistungsaufnahme (in Watt).

Vorwarn Schwellwert

Schwellwert als prozentualer Wert der unter *Verbrauch begrenzen* angegebenen maximalen Leistungsaufnahme. Bei Erreichen des Schwellwertes wird die unter *Aktion bei Überschreitung* festgelegte Aktion ausgeführt.

Überschreitung Toleranz Zeit

Zeitspanne (in Minuten), die nach Erreichen des Schwellwerts gewartet werden soll, bevor die Aktion ausgeführt wird.

Aktion bei Überschreitung

Aktion, die bei Erreichen des Schwellwerts nach Ablauf der Toleranzzeit ausgeführt wird:

Keine Aktion

Es wird keine Aktion ausgeführt.

System Herunterfahren (Shutdown)

System „sanft“ herunterfahren und ausschalten.

Diese wird nur unterstützt, wenn ServerView-Agenten installiert und beim iRMC S2/S3 als „Connected“ gemeldet sind.

Sofort Ausschalten

Der Server unabhängig wird vom Status des Betriebssystems sofort ausgeschaltet.

Dynamische Steuerung aktiviert

Die Energieverbrauchsbegrenzung wird dynamisch gesteuert.

7.8.2 Aktueller System Energieverbrauch - aktuellen Energieverbrauch anzeigen

Diese Anzeige wird nicht von allen PRIMERGY Servern mit iRMC S2/S3 unterstützt.

Auf der Seite *Aktueller Energieverbrauch* wird der aktuelle Stromverbrauch der Systemkomponenten sowie des Gesamtsystems angezeigt.

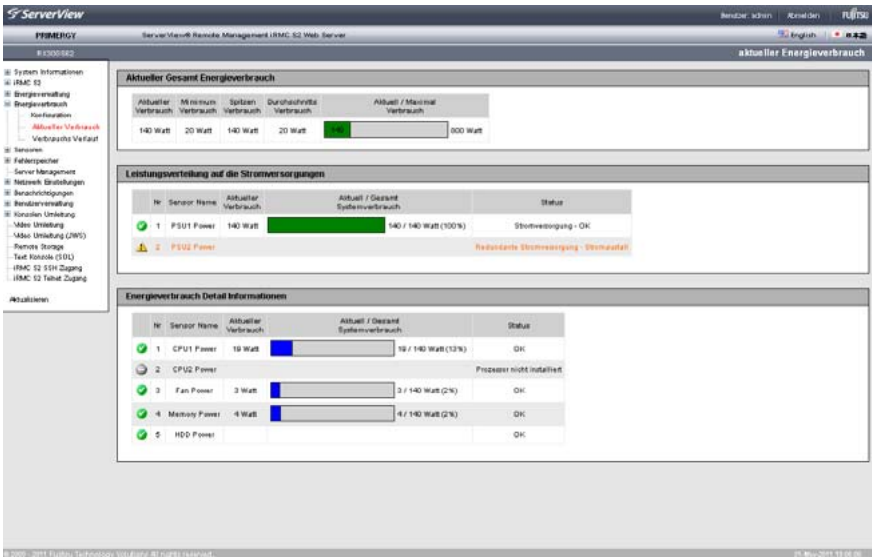


Bild 113: Seite Aktueller Energieverbrauch

7.8.3 Energieverbrauch Verlauf - zeitlichen Verlauf des Energieverbrauchs anzeigen

Auf der Seite *Energieverbrauch Verlauf* können Sie sich den zeitlichen Verlauf des Energieverbrauchs Ihres PRIMERGY Servers grafisch anzeigen lassen.

Diese Anzeige wird nicht von allen PRIMERGY Servern mit iRMC S2/S3 unterstützt.

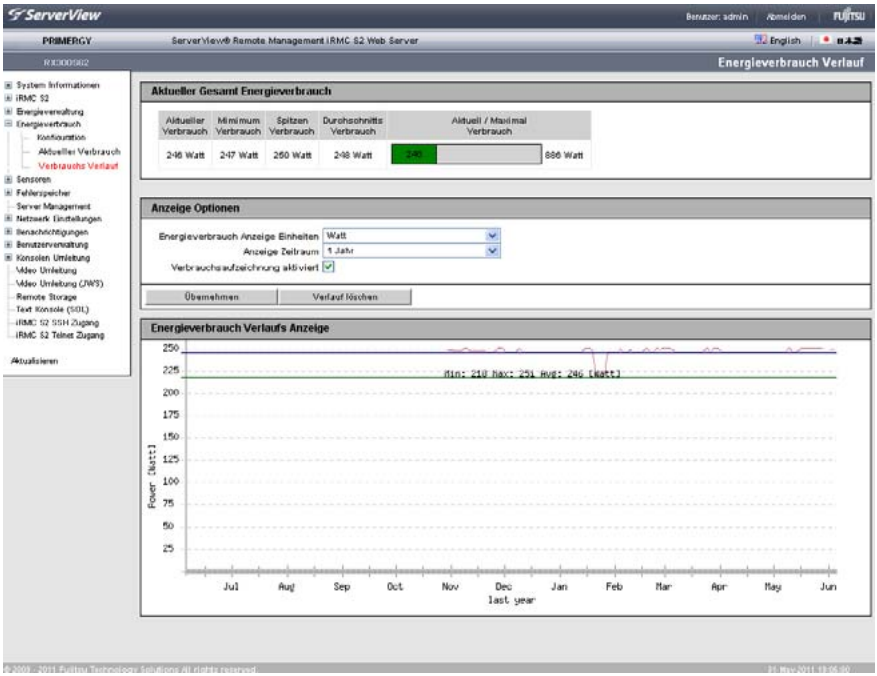


Bild 114: Seite Energieverbrauch Verlauf

Aktueller Gesamt Energieverbrauch

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

Unter *Aktueller Gesamt Energieverbrauch* werden die Messwerte zum aktuellen, minimalen, maximalen sowie durchschnittlichen Energieverbrauch des verwalteten Servers im aktuellen Intervall angezeigt.

In einer grafischen Anzeige wird außerdem der aktuelle Energieverbrauch des Servers der maximal möglichen Leistungsaufnahme gegenübergestellt.

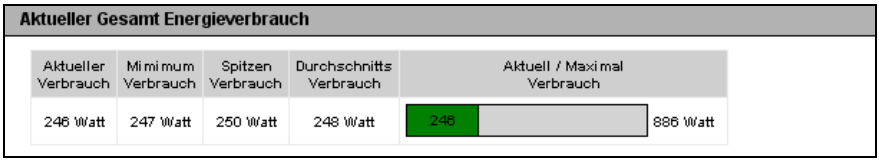


Bild 115: Seite Energieverbrauch Verlauf - Aktueller Gesamt Energieverbrauch

Anzeige Optionen

Unter *Anzeige Optionen* spezifizieren Sie die Parameter für die Anzeige des Energieverbrauchsverlaufs.

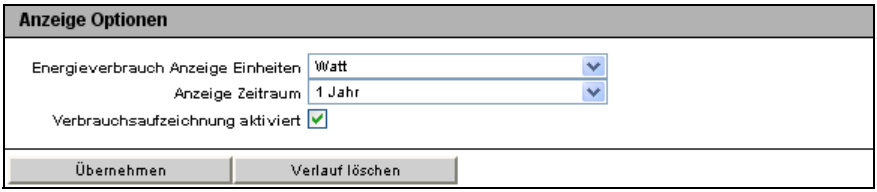


Bild 116: Seite Energieverbrauch Verlauf -Anzeige Optionen

Energie Verbrauch Anzeige Einheiten

Einheit der elektrischen Leistung:

- *Watt*
- *BTU/h* (British Thermal Unit/hour, 1 BTU/h entspricht 0,293 Watt).

Anzeige Zeitraum

Zeitintervall, für das der Leistungsverbrauch grafisch dargestellt wird.

Folgende Intervalle stehen zur Auswahl:

1 Stunde

Standardwert.
Die Messwerte der letzten Stunde (60 Werte). Da jede Minute ein Messwert erzeugt wird, werden somit alle Messwerte der letzten Stunde angezeigt.

12 Stunden

Die Messwerte der letzten 12 Stunden. Es wird ein Messwert pro einem Zeitabschnitt von fünf Minuten dargestellt (jeder 5. Messwert, insgesamt 144 Werte).

1 Tag

Die Messwerte der letzten 24 Stunden. Es wird ein Messwert pro einem Zeitabschnitt von 10 Minuten dargestellt (jeder 10. Messwert, insgesamt 144 Werte)

1 Woche

Die Messwerte der letzten Woche. Es wird ein Messwert pro Stunde dargestellt (jeder 60. Messwert, insgesamt 168 Werte).

2 Wochen

Die Messwerte der letzten beiden Wochen. Es wird ein Messwert pro Zeitabschnitt von zwei Stunden dargestellt (jeder 120. Messwert, insgesamt 168 Werte).

1 Monat

Die Messwerte des letzten Monats. Es wird ein Messwert pro einem Zeitabschnitt von ungefähr vier Stunden dargestellt (jeder 240. Messwert, insgesamt 180 Werte).

1 Jahr

Die Messwerte der letzten 12 Monate. Es wird ein Messwert pro einem Zeitabschnitt von zwei Tagen dargestellt (jeder 2880. Messwert, insgesamt 180 Werte).

Verbrauchsaufzeichnung aktiviert

Wenn Sie diese Option aktivieren, wird der zeitliche Verlauf des Energieverbrauchs aufgezeichnet.

Verbrauchsaufzeichnung (Power Monitoring) ist ab Firmware Version 3.32 standardmäßig aktiviert.

Diese Einstellung ist nur wirksam bei PRIMERGY Servern, die Verbrauchsaufzeichnung unterstützen.

- Klicken Sie auf die Schaltfläche *Übernehmen*, und Ihre Einstellungen zu aktivieren.
- Zum Löschen der angezeigten Daten klicken Sie auf die Schaltfläche *Verlauf löschen*.

Energie Verbrauch Verlaufs Anzeige

Unter *Energieverbrauch Verlaufs Anzeige* wird der zeitliche Verlauf des Energieverbrauchs des verwalteten Servers in einem Kurvendiagramm dargestellt (entsprechend den Einstellungen unter *Anzeige Optionen*). Der tatsächlich angefallene Energieverbrauch kann vom angezeigten Energieverbrauch ungefähr 20% abweichen.

Bild 117: Energieverbrauch Verlauf - Energie Verbrauch Verlaufs Anzeige

7.9 Sensoren - Status der Sensoren überprüfen

Unter dem Eintrag „Sensoren“ stehen Ihnen Seiten zur Verfügung, mit denen Sie die Sensoren des verwalteten Servers überprüfen können:

– "Lüfter - Lüfter überprüfen" auf Seite 219.

– "Temperatur - Temperatursensoren überprüfen" auf Seite 221.

– "Spannungen - Spannungssensoren überprüfen" auf Seite 223.

– "Netzteil - Stromversorgung überprüfen" auf Seite 224.

– "Komponenten Status - Status der Serverkomponenten überprüfen" auf Seite 226.

Um die Statusüberprüfung zu erleichtern, wird der Status eines Sensors nicht nur über seinen aktuellen Wert angezeigt, sondern außerdem über Farbcode und Status-Icon:

Schwarz /	Der gemessene Wert liegt innerhalb des im Betriebszustand normalen Wertebereichs.
Orange /	Der gemessene Wert übersteigt die Warnschwelle. Der Systembetrieb ist aber noch nicht gefährdet.
Rot /	Der gemessene Wert übersteigt die kritische Schwelle. Der Systembetrieb kann gefährdet sein und die Datenintegrität könnte bedroht sein.

Tabelle 6: Status der Sensoren

7.9.1 Lüfter - Lüfter überprüfen

Die Seite *Lüfter* informiert über Lüfter und deren Status.

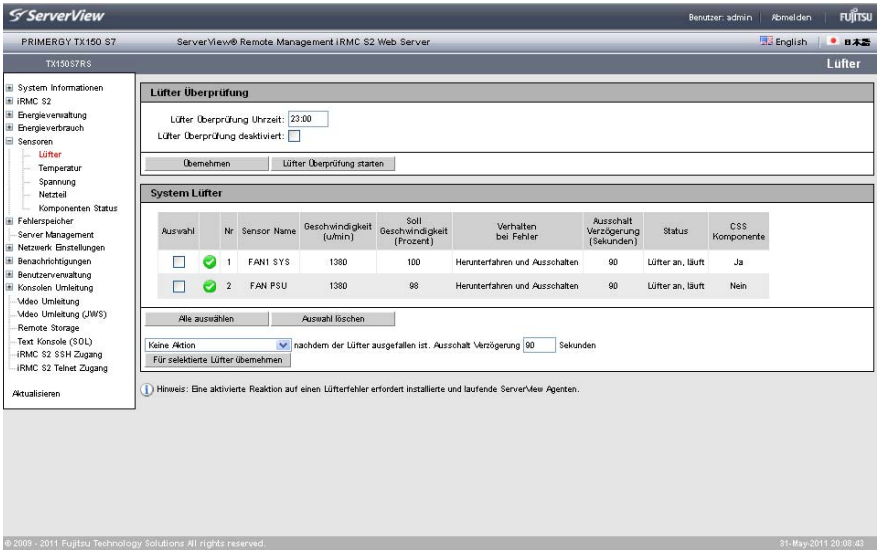


Bild 118: Seite Lüfter

Lüfter Überprüfung - Lüfter testen

Mit der Gruppe *Lüfter überprüfen* können Sie einen Zeitpunkt für einen automatischen Start der Lüfter-Überprüfung festlegen oder die Überprüfung der Lüfter explizit starten.

Anstatt die Tests wie früher mit voller Lüfterdrehzahl durchzuführen, führen die meisten Systeme den Lüftertest nun mit einer Drehzahl nahe der aktuell benötigten Drehzahl durch. In diesem Fall macht sich der Lüftertest nicht mehr akustisch bemerkbar.

Lüftertest Uhrzeit

Tragen Sie hier den Zeitpunkt für einen automatischen Start der Lüfter-Überprüfung ein.

Lüfter überprüfung deaktiviert

Wenn Sie diese Option wählen, ist die Lüfterprüfung deaktiviert.

- ► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.
- ► Klicken Sie auf die Schaltfläche *Überprüfung starten,* wenn Sie die Lüfter-Überprüfung explizit starten wollen.

System Lüfter - Server-Verhalten bei Ausfall von Lüftern festlegen

Mit der Gruppe *System Lüfter* können Sie sich über den Status der Lüfter informieren. Dabei können Sie via Option oder Schaltfläche einzelne oder alle Lüfter auswählen und festlegen, ob bei Ausfall dieser Lüfter der Server nach einer spezifizierten Anzahl von Sekunden heruntergefahren werden soll.

Alle auswählen
: Alle Lüfter werden ausgewählt.

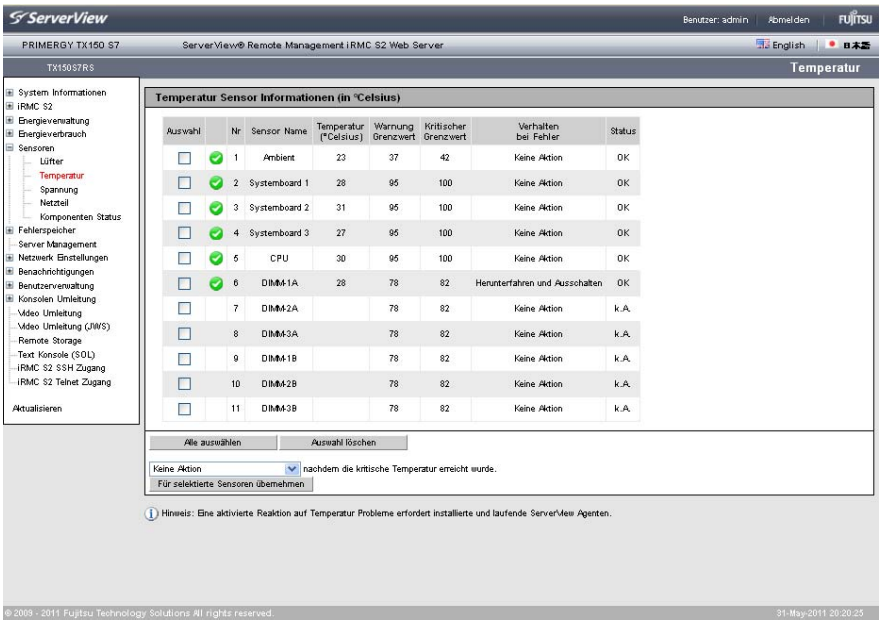
Auswahl löschen
: Alle Auswahlmarkierungen werden gelöscht.

- ► Markieren Sie die Lüfter, für die Sie ein Verhalten im Fehlerfall definieren wollen.
- ► Definieren Sie das Verhalten im Fehlerfall über die Liste am unteren Ende des Arbeitsbereichs:
  - – Wählen Sie *Keine Aktion*, wenn bei Ausfall der ausgewählten Lüfter der der Server nicht heruntergefahren werden soll.
  - – Wählen Sie *Herunterfahren und Ausschalten*, wenn bei Ausfall der ausgewählten Lüfter der Server heruntergefahren und ausgeschaltet werden soll. Spezifizieren Sie in diesem Fall außerdem im Eingabefeld *Ausschalt Verzögerung* die gewünschten Zeitspanne (in Sekunden) zwischen dem Ausfall des Lüfters und dem Herunterfahren des Servers.

    Bei redundanten Lüftern wird der Server erst dann heruntergefahren, wenn mehr als ein Lüfter defekt ist und für diese Lüfter außerdem *Herunterfahren und Ausschalten* eingestellt ist.
- ► Klicken Sie auf die Schaltfläche *Für selektierte Lüfter übernehmen,* um Ihre Einstellungen für die ausgewählten Lüfter zu aktivieren.

7.9.2 Temperatur - Temperatursensoren überprüfen

Die Seite *Temperatur* informiert über den Status der Temperatursensoren, die die Temperatur an Serverkomponenten wie z. B CPU oder FBD (Fully buffered DIMM) sowie die Umgebungstemperatur messen.


ServerView
Benutzer: admin | Abmelden | FUJITSU
PRIMERGY TX150 S7
ServerView® Remote Management iRMC S2 Web Server
English
TX150S7RS
Temperatur
System Informationen
iRMC S2
Energieverwaltung
Energieverbrauch
Sensoren
Lüfter
Temperatur
Spannung
Netzteil
Komponenten Status
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigungen
Benutzerverwaltung
Konsolen Umleitung
Video Umleitung
Video Umleitung (JWS)
Remote Storage
Text Konsole (SOL)
iRMC S2 SSH Zugang
iRMC S2 Telnet Zugang
Aktualisieren
Temperatur Sensor Informationen (in °Celsius)
Auswahl | Nr | Sensor Name | Temperatur (°Celsius) | Warnung Grenzwert | Kritischer Grenzwert | Verhalten bei Fehler | Status
1 Ambient 23 37 42 Keine Aktion OK
2 Systemboard 1 28 95 100 Keine Aktion OK
3 Systemboard 2 31 95 100 Keine Aktion OK
4 Systemboard 3 27 95 100 Keine Aktion OK
5 CPU 30 95 100 Keine Aktion OK
6 DIMM-1A 28 78 82 Herunterfahren und Ausschalten OK
7 DIMM-2A 78 82 Keine Aktion k.A.
8 DIMM-3A 78 82 Keine Aktion k.A.
9 DIMM-1B 78 82 Keine Aktion k.A.
10 DIMM-2B 78 82 Keine Aktion k.A.
11 DIMM-3B 78 82 Keine Aktion k.A.
Alle auswählen
Auswahl löschen
Keine Aktion
nachdem die kritische Temperatur erreicht wurde.
Für selektierte Sensoren übernehmen
Hinweis: Eine aktivierte Reaktion auf Temperatur Probleme erfordert installierte und laufende ServerView Agenten.
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
31-May-2011 20:20:25
Bild 119: Seite Temperatur

Via Option oder Schaltfläche können Sie einzelne oder alle Temperatursensoren auswählen und festlegen, ob bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Server heruntergefahren werden soll.

Alle auswählen
: Alle Temperatursensoren werden ausgewählt.

Auswahl löschen
: Alle Auswahlmarkierungen werden gelöscht.

► Markieren Sie die Sensoren, für die Sie ein Verhalten bei Erreichen der kritischen Temperatur definieren wollen.

- Definieren Sie das Verhalten bei Erreichen der kritischen Temperatur über die Liste am unteren Ende des Arbeitsbereichs:
  - Wählen Sie *Keine Aktion*, wenn bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Shutdown des Servers nicht eingeleitet werden soll.
  - Wählen Sie *Herunterfahren und Ausschalten*, wenn bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Server heruntergefahren und ausgeschaltet werden soll.
- Klicken Sie auf die Schaltfläche *Für selektierte Sensoren übernehmen,* um Ihre Einstellungen für die ausgewählten Temperatursensoren zu aktivieren.

7.9.3 Spannungen - Spannungssensoren überprüfen

Die Seite *Spannungen* informiert über den Status von Spannungssensoren, die den Serverkomponenten zugeordnet sind.

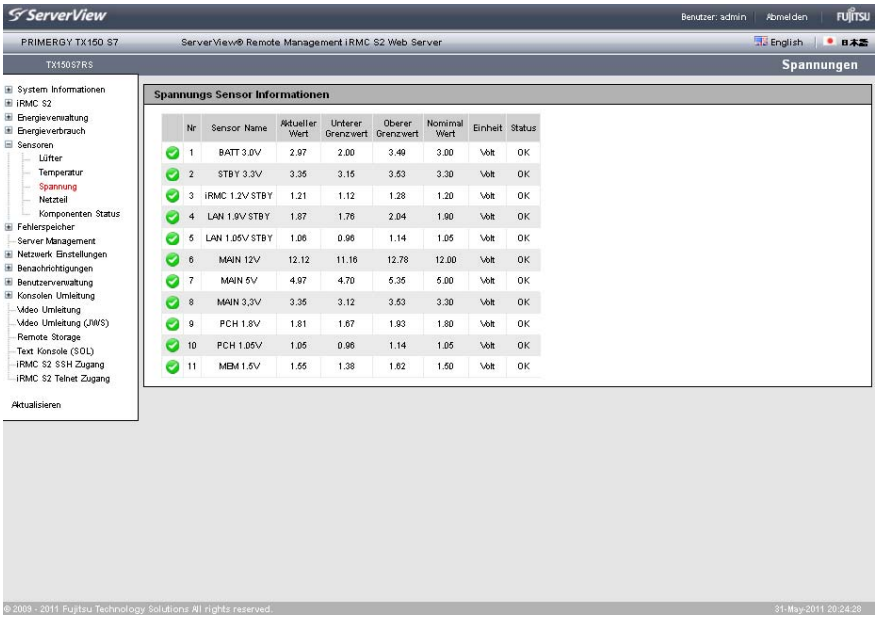


Bild 120: Seite Spannungen

7.9.4 Netzteil - Stromversorgung überprüfen

Die Seite *Netzteil* informiert über den Zustand der Stromversorgung durch die Netzgeräte. Für einige Server-Typen können Sie auf der Seite *Netzteil* außerdem die Einstellungen für die redundante Stromversorgung konfigurieren.

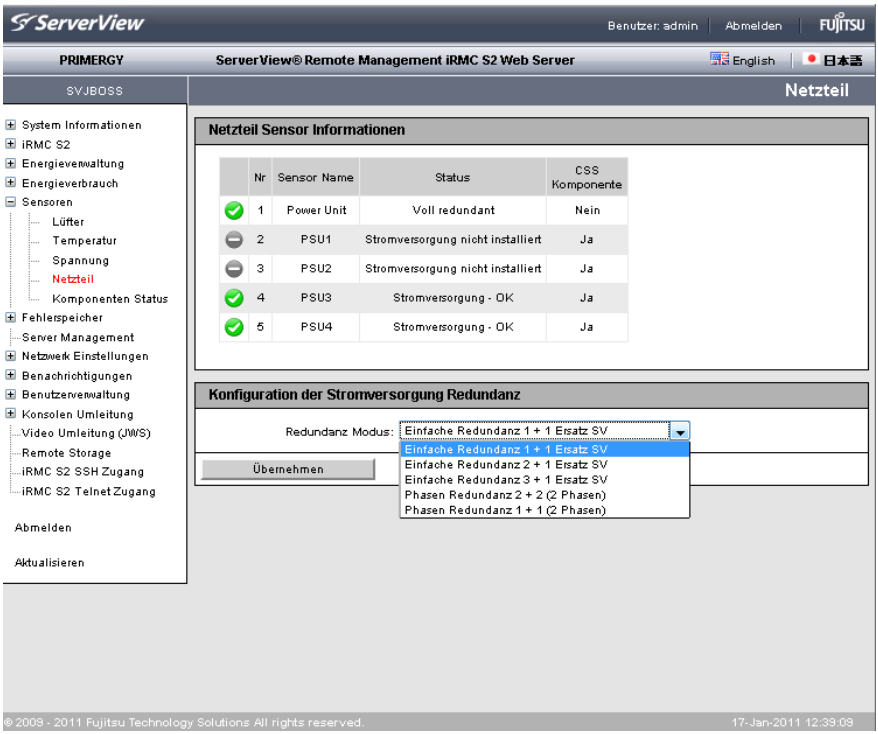


Bild 121: Seite Netzteil

Redundante Stromversorgung konfigurieren

Diese Funktion ist nicht bei allen Server verfügbar.

In der Gruppe *Konfiguration der redundanten Stromversorgung* können Sie Redundanz-Modus für die Stromversorgung am verwalteten Server einstellen. Welche der nachfolgenden Optionen tatsächlich verfügbar ist, hängt von den Eigenschaften des jeweiligen Servers ab.

Einfache Redundanz 1 + 1 Ersatz SV
: Systembetrieb ist garantiert für den Ausfall eines Netzteils bei insgesamt zwei Netzteilen.

Einfache Redundanz 2 + 1 Ersatz SV
: Systembetrieb ist garantiert für den Ausfall eines Netzteils bei insgesamt drei Netzteilen.

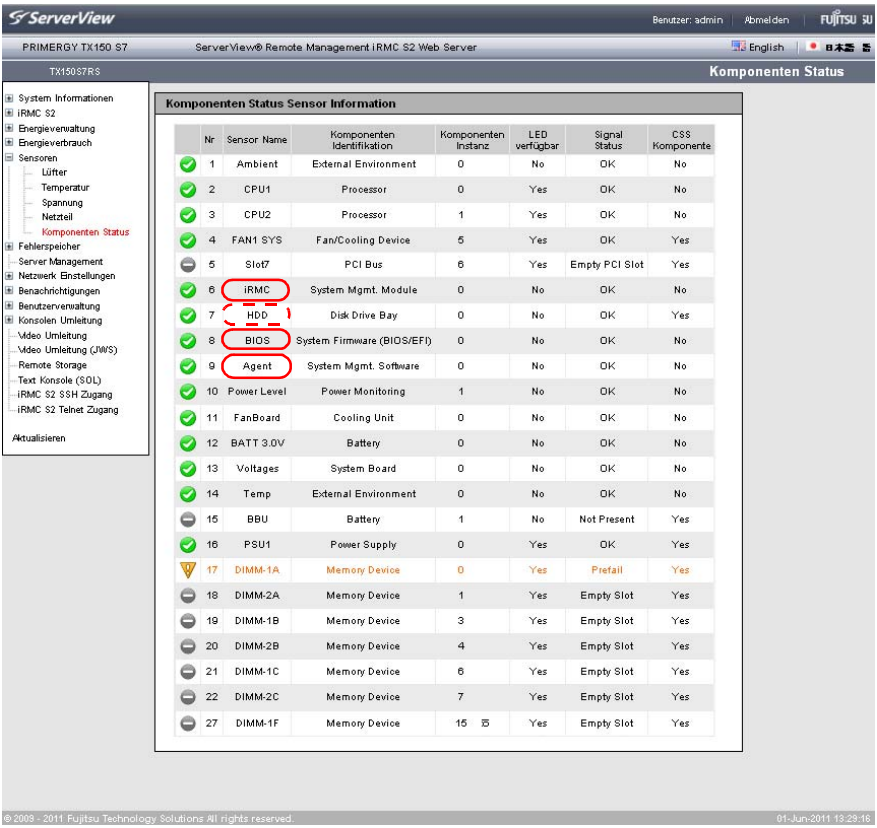
Einfache Redundanz 3 + 1 Ersatz SV
: Systembetrieb ist garantiert für den Ausfall eines Netzteils bei insgesamt vier Netzteilen.

Phasen Redundanz 2 + 2 (2 Phasen)
: Zwei der vier Netzteile sind jeweils an eine separate Wechselstromquelle angeschlossen. Dies garantiert die Aufrechterhaltung des Systembetriebs selbst bei Ausfall einer Stromleitung oder eines einzelnen Netzteils.

Phasen Redundanz 1+ 1 (2 Phasen)
: Jedes von insgesamt zwei Netzteilen ist an eine separate Wechselstromquelle angeschlossen. Dies garantiert die Aufrechterhaltung des Systembetriebs selbst bei Ausfall einer Stromleitung oder eines einzelnen Netzteils.

7.9.5 Komponenten Status - Status der Serverkomponenten überprüfen

Die Seite *Komponenten Status* informiert über den Status der Serverkomponenten. In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice)-Funktionalität unterstützt wird.


ServerView
Benutzer: admin | Abmelden | FUJITSU
PRIMERGY TX150 S7
ServerView® Remote Management iRMC S2 Web Server
English
TX150S7RS
Komponenten Status
System Informationen
iRMC S2
Energieverwaltung
Energieverbrauch
Sensoren
Lüfter
Temperatur
Spannung
Netzteil
Komponenten Status
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigungen
Benutzerverwaltung
Konsolen Umleitung
Video Umleitung
Video Umleitung (JWS)
Remote Storage
Text Konsole (SOL)
iRMC S2 SSH Zugang
iRMC S2 Telnet Zugang
Aktualisieren
Komponenten Status Sensor Information
Nr | Sensor Name | Komponenten Identifikation | Komponenten Instanz | LED verfügbar | Signal Status | CSS Komponente
1 | Ambient | External Environment | 0 | No | OK | No
2 | CPU1 | Processor | 0 | Yes | OK | No
3 | CPU2 | Processor | 1 | Yes | OK | No
4 | FAN1 SYS | Fan/Cooling Device | 5 | Yes | OK | Yes
5 | Slot7 | PCI Bus | 6 | Yes | Empty PCI Slot | Yes
6 | iRMC | System Mgmt. Module | 0 | No | OK | No
7 | HDD | Disk Drive Bay | 0 | No | OK | Yes
8 | BIOS | System Firmware (BIOS/EFI) | 0 | No | OK | No
9 | Agent | System Mgmt. Software | 0 | No | OK | No
10 | Power Level | Power Monitoring | 1 | No | OK | No
11 | FanBoard | Cooling Unit | 0 | No | OK | No
12 | BATT 3.0V | Battery | 0 | No | OK | No
13 | Voltages | System Board | 0 | No | OK | No
14 | Temp | External Environment | 0 | No | OK | No
15 | BBU | Battery | 1 | No | Not Present | Yes
16 | PSU1 | Power Supply | 0 | Yes | OK | Yes
17 | DIMM-1A | Memory Device | 0 | Yes | Prefail | Yes
18 | DIMM-2A | Memory Device | 1 | Yes | Empty Slot | Yes
19 | DIMM-1B | Memory Device | 3 | Yes | Empty Slot | Yes
20 | DIMM-2B | Memory Device | 4 | Yes | Empty Slot | Yes
21 | DIMM-1C | Memory Device | 6 | Yes | Empty Slot | Yes
22 | DIMM-2C | Memory Device | 7 | Yes | Empty Slot | Yes
27 | DIMM-1F | Memory Device | 15 | Yes | Empty Slot | Yes
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
01-Jun-2011 13:29:16
Bild 122: Seite Komponenten Status

Einträge mit Sensor Name "iRMC", "Agent", "BIOS" oder "VIOM"

Einträge mit *Sensor Name* "iRMC", "Agent", "BIOS" oder "VIOM" weist darauf hin, dass iRMC S2/S3, Agent oder BIOS einen Fehler entdeckt haben. Es bedeutet nicht, dass iRMC S2/S3, Agent, BIOS oder VIOM selbst fehlerhaft sind

Einträge mit Sensor Name "HDD"und "HDD<n> und "agentless" HDD Monitoring ("out-of-band" HDD Monitoring)

Einträge mit *Sensor Name* "HDD" oder "HDD<n>" (mit n = 1, 2, ...) zeigen die Status von Festplatten-Laufwerken (Hard Disk Drives, HDD) an:

– Der Eintrag mit *Sensor Name* "HDD" zeigt den Gesamtstatus über alle HDDs des Servers als Zusammenfassung der Status der einzelnen HDDs an.

  Der HDD-Gesamtstatus des Servers wird von den ServerView-Agenten und dem ServerView RAID Manager ausgelesen und an den iRMC S3 gemeldet.

– Ein Eintrag mit *Sensor Name* "HDD<n>" (mit n = 1, 2, ...) zeigt den Status eines einzelnen HDD an.

Beachten Sie

– Diese Funktionalität wird nur vom iRMC S3 unterstützt.

– Diese Funktionalität wird nur unterstützt, wenn der verwaltete PRIMERGY Server das "agentless" HDD Monitoring (auch "Out-of-band HDD Monitoring" genannt) unterstützt.

Wenn diese Voraussetzungen erfüllt sind, wird der HDD<n>-Status jedes einzelnen HDD direkt, d.h. ohne Nutzung der ServerView-Agenten an den iRMC S3 gemeldet.

✓	59	HDD1	Disk Drive Bay	1	No	OK	Yes
⚠	60	HDD2	Disk Drive Bay	2	No	Prefail	Yes
✗	61	HDD3	Disk Drive Bay	3	No	Failed	Yes
✓	62	HDD4	Disk Drive Bay	4	No	OK	Yes

Bild 123: Statusanzeige für einzelne Festplatten-Laufwerke (HDDs)

Welche Einträge genau in der Tabelle *Komponenten Status Sensor Information* angezeigt werden, hängt deshalb vom Zustand des Servers ab, und ob der Server "agentless" HDD Monitoring unterstützt:

- Der Eintrag mit *Sensor Name* "HDD" zeigt nur dann einen Status in der Spalte *Signal Status* an, wenn die ServerView-Agenten und der ServerView RAID Manager auf dem verwalteten Server installiert sind und ausgeführt werden. Andernfalls wird stattdessen "N/A" (not available) in der Spalte *Signal Status* angezeigt.
- Die Einträge mit *Sensor Name* "HDD<n> (mit n = 1, 2, ...)" werden nur angezeigt wenn der verwaltete Server "agentless" HDD Monitoring unterstützt.

7.10 Fehlerspeicher und interner Ereignisspeicher

Der Eintrag *Fehlerspeicher* enthält die Verweise auf die Seiten zur Anzeige und Konfiguration des IPMI-Fehlerspeichers (System Eventlog, SEL) und des internen Ereignisspeichers des Servers:

– "IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge" auf Seite 230.

  Die Einträge des IPMI-Fehlerspeichers liefern Informationen zu Ereignissen wie Betriebssystem-Boots / Shutdowns, Lüfterfehler und iRMC S2/S3-Firmware-Aktualisierungen.

– "IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge" auf Seite 230.

  Die Einträge des internen Fehlerspeichers liefern Informationen zu Audit-Ereignissen (Login-Events, Herstellen einer AVR-Verbindung usw.) sowie zusätzliche Informationen (z.B. IPv6-relevante Informationen und LDAP-Benutzernamen).

– "Fehlerspeicher Konfiguration - IPMI SEL und internen Ereignisspeicher konfigurieren" auf Seite 236.

Zur besseren Übersichtlichkeit sind den einzelnen Ereignis-/Fehlerkategorien farbige Icons zugeordnet:

	Kritischer Fehler
	Schwerer Fehler
	Leichter Fehler
	Information
	Customer Self Service (CSS)-Ereignis

Tabelle 7: Ereigniskategorien der Fehlerliste

7.10.1 IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge

Die Seite *Fehlerliste* informiert über den IPMI-Fehlerspeicher und zeigt die Einträge des IPMI-Fehlerspeichers) an. Die Einträge des IPMI-Fehlerspeichers liefern Informationen zu Ereignissen wie Betriebssystem-Boots / Shutdowns, Lüfterfehler und iRMC S2/S3-Firmware-Aktualisierungen.

In der Spalte *CSS Komponente* ist für die einzelnen Ereignisse vermerkt, ob das Ereignis von einer CSS (**C**ustomer **S**elf **S**ervice)-Komponente ausgelöst wurde.

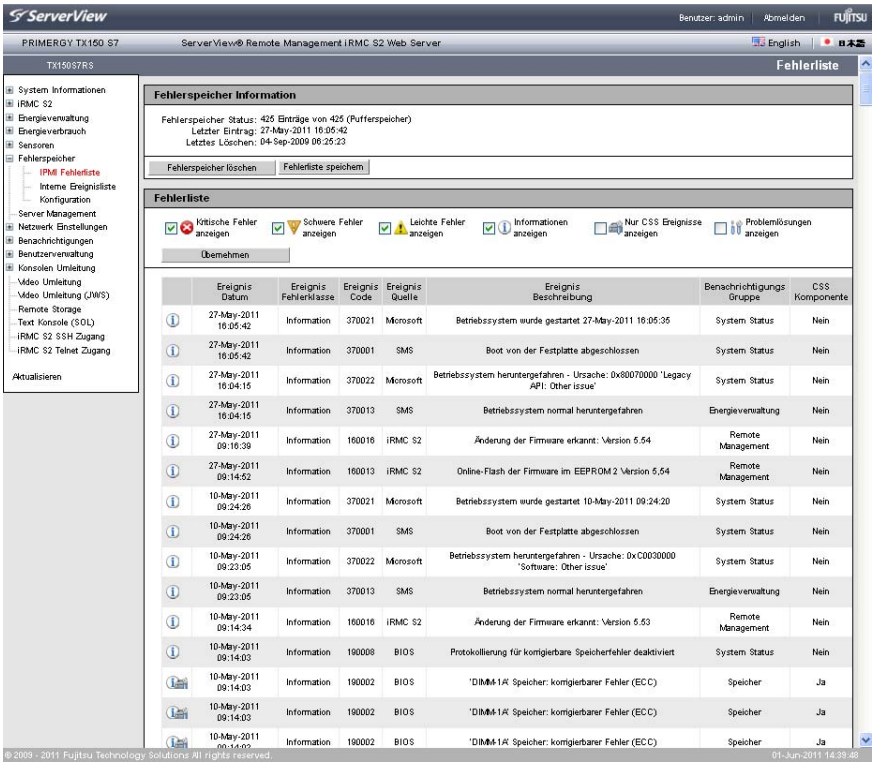

ServerView
Benutzer: admin | Abmelden | FUJITSU
PRIMERGY TX150 S7
ServerView® Remote Management iRMC S2 Web Server
English
TX150S7RS
Fehlerliste
System Informationen
iRMC S2
Energieverwaltung
Energieverbrauch
Sensoren
Fehlerspeicher
IPMI Fehlerliste
Interne Ereignisliste
Konfiguration
Server Management
Netzwerk Einstellungen
Benachrichtigungen
Benutzerverwaltung
Konsolen Umleitung
Video Umleitung
Video Umleitung (JWS)
Remote Storage
Text Konsole (SOL)
iRMC S2 SSH Zugang
iRMC S2 Telnet Zugang
Aktualisieren
Fehlerspeicher Information
Fehlerspeicher Status: 426 Einträge von 426 (Pufferspeicher)
Letzter Eintrag: 27-May-2011 16:05:42
Letztes Löschen: 04-Sep-2009 06:25:23
Fehlerspeicher löschen
Fehlerliste speichern
Fehlerliste
Kritische Fehler anzeigen
Schwere Fehler anzeigen
Leichte Fehler anzeigen
Informationen anzeigen
Nur CSS Ereignisse anzeigen
Problemlösungen anzeigen
Übernehmen
Ereignis Datum
Ereignis Fehlerklasse
Ereignis Code
Ereignis Quelle
Ereignis Beschreibung
Benachrichtigungs Gruppe
CSS Komponente
27-May-2011 16:05:42 | Information | 370021 | Microsoft | Betriebssystem wurde gestartet 27-May-2011 16:05:35 | System Status | Nein
27-May-2011 16:05:42 | Information | 370001 | SMS | Boot von der Festplatte abgeschlossen | System Status | Nein
27-May-2011 16:04:15 | Information | 370022 | Microsoft | Betriebssystem heruntergefahren - Ursache: 0x80070000 'Legacy API: Other issue' | System Status | Nein
27-May-2011 16:04:15 | Information | 370013 | SMS | Betriebssystem normal heruntergefahren | Energieverwaltung | Nein
27-May-2011 09:16:39 | Information | 160016 | iRMC S2 | Änderung der Firmware erkannt: Version 5.54 | Remote Management | Nein
27-May-2011 09:14:52 | Information | 160013 | iRMC S2 | Online-Flash der Firmware im EEPROM 2 Version 5.54 | Remote Management | Nein
10-May-2011 09:24:26 | Information | 370021 | Microsoft | Betriebssystem wurde gestartet 10-May-2011 09:24:20 | System Status | Nein
10-May-2011 09:24:26 | Information | 370001 | SMS | Boot von der Festplatte abgeschlossen | System Status | Nein
10-May-2011 09:23:05 | Information | 370022 | Microsoft | Betriebssystem heruntergefahren - Ursache: 0xC0030000 'Software: Other issue' | System Status | Nein
10-May-2011 09:23:05 | Information | 370013 | SMS | Betriebssystem normal heruntergefahren | Energieverwaltung | Nein
10-May-2011 09:14:34 | Information | 160016 | iRMC S2 | Änderung der Firmware erkannt: Version 5.53 | Remote Management | Nein
10-May-2011 09:14:03 | Information | 190008 | BIOS | Protokollierung für korrigierbare Speicherfehler deaktiviert | System Status | Nein
10-May-2011 09:14:03 | Information | 190002 | BIOS | 'DIMM-1A' Speicher: korrigierbarer Fehler (ECC) | Speicher | Ja
10-May-2011 09:14:03 | Information | 190002 | BIOS | 'DIMM-1A' Speicher: korrigierbarer Fehler (ECC) | Speicher | Ja
10-May-2011 09:14:03 | Information | 190002 | BIOS | 'DIMM-1A' Speicher: korrigierbarer Fehler (ECC) | Speicher | Ja
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
01-Jun-2011 14:39:40

Bild 124: Seite Fehlerliste

Fehlerspeicher Information

Die Gruppe *Fehlerspeicher Information* informiert über Füllgrad / die Anzahl der Einträge des Fehlerspeichers. Außerdem ist vermerkt, wann zuletzt Einträge hinzugefügt oder gelöscht wurden.

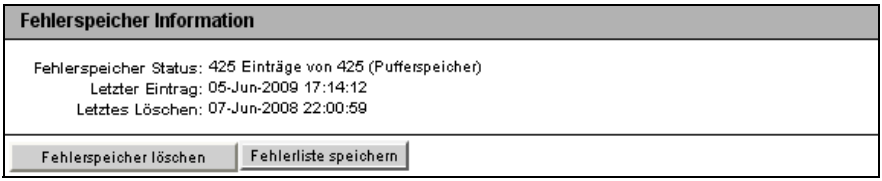


Bild 125: Seite Fehlerliste - Fehlerspeicher Information

Fehlerspeicher löschen

Durch Klicken auf *Fehlerspeicher löschen* löschen Sie alle Einträge im Fehlerspeicher.

Fehlerliste speichern

Nach dem Klicken auf *Fehlerliste speichern* bietet Ihnen der iRMC S2/S3 die Datei *iRMC S2/S3_EventLog.sel*, in der die Fehlerspeicher-Einträge enthalten sind, zum Herunterladen an.

IPMI-Fehlerliste

In der Gruppe *Fehlerliste* werden die Fehlerspeicher-Einträge – nach Ereigniskategorien gefiltert – angezeigt.

In der Gruppe *Fehlerliste* können Sie die Filterkriterien für die Dauer der aktuellen Sitzung modifizieren. Die hier vorgenommenen Einstellungen sind jedoch nur bis zum nächsten Abmelden wirksam. Danach gelten wieder die Standardeinstellungen.

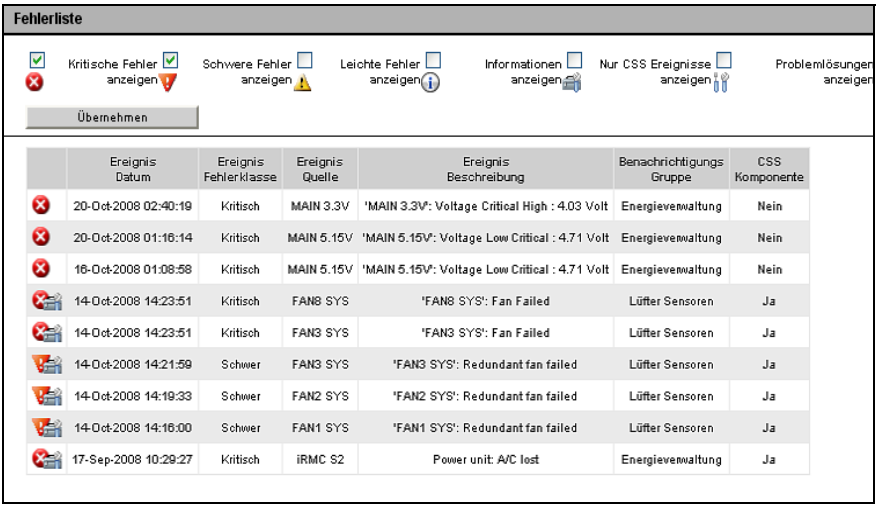

Fehlerliste
Kritische Fehler anzeigen
Schwere Fehler anzeigen
Leichte Fehler anzeigen
Informationen anzeigen
Nur CSS Ereignisse anzeigen
Problemlösungen anzeigen
Übernehmen
Ereignis Datum
Ereignis Fehlerklasse
Ereignis Quelle
Ereignis Beschreibung
Benachrichtigungs Gruppe
CSS Komponente
20-Oct-2008 02:40:19 Kritisch MAIN 3.3V 'MAIN 3.3V': Voltage Critical High : 4.03 Volt Energieverwaltung Nein
20-Oct-2008 01:16:14 Kritisch MAIN 5.15V 'MAIN 5.15V': Voltage Low Critical : 4.71 Volt Energieverwaltung Nein
16-Oct-2008 01:08:58 Kritisch MAIN 5.15V 'MAIN 5.15V': Voltage Low Critical : 4.71 Volt Energieverwaltung Nein
14-Oct-2008 14:23:51 Kritisch FAN8 SYS 'FAN8 SYS': Fan Failed Lüfter Sensoren Ja
14-Oct-2008 14:23:51 Kritisch FAN3 SYS 'FAN3 SYS': Fan Failed Lüfter Sensoren Ja
14-Oct-2008 14:21:59 Schwer FAN3 SYS 'FAN3 SYS': Redundant fan failed Lüfter Sensoren Ja
14-Oct-2008 14:19:33 Schwer FAN2 SYS 'FAN2 SYS': Redundant fan failed Lüfter Sensoren Ja
14-Oct-2008 14:16:00 Schwer FAN1 SYS 'FAN1 SYS': Redundant fan failed Lüfter Sensoren Ja
17-Sep-2008 10:29:27 Kritisch iRMC S2 Power unit: A/C lost Energieverwaltung Ja

Bild 126: Seite Fehlerliste - Gruppe Fehleriste

Kritische Fehler anzeigen, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*, *Nur CSS Ereignisse anzeigen*

Wählen Sie hier gegebenenfalls ein oder mehrere, von der Standardkonfiguration abweichende Fehlerkategorien aus.

Problemlösungen anzeigen

Wenn Sie diese Option wählen, wird zu jedem Fehlerspeicher-Eintrag der Fehlerkategorien *Kritischer Fehler* und *Schwerer Fehler* ein Lösungsvorschlag angezeigt.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen für die Dauer der aktuellen Sitzung zu aktivieren.

7.10.2 Interne Ereignisliste - Information zum internen Ereignisspeicher und Anzeige der Einträge

Die Seite *Interner Ereignis Speicher Information* liefert Informationen zum internen Ereignisspeicher und zeigt die zugehörigen Einträge (interne Ereignisliste) an. Der interne Ereignisspeicher umfasst Informationen zu Audit-Ereignissen (Login-Events, Herstellen einer AVR-Verbindung usw.) sowie zusätzliche Informationen (z.B. IPv6-relevante Informationen und LDAP-Benutzernamen).

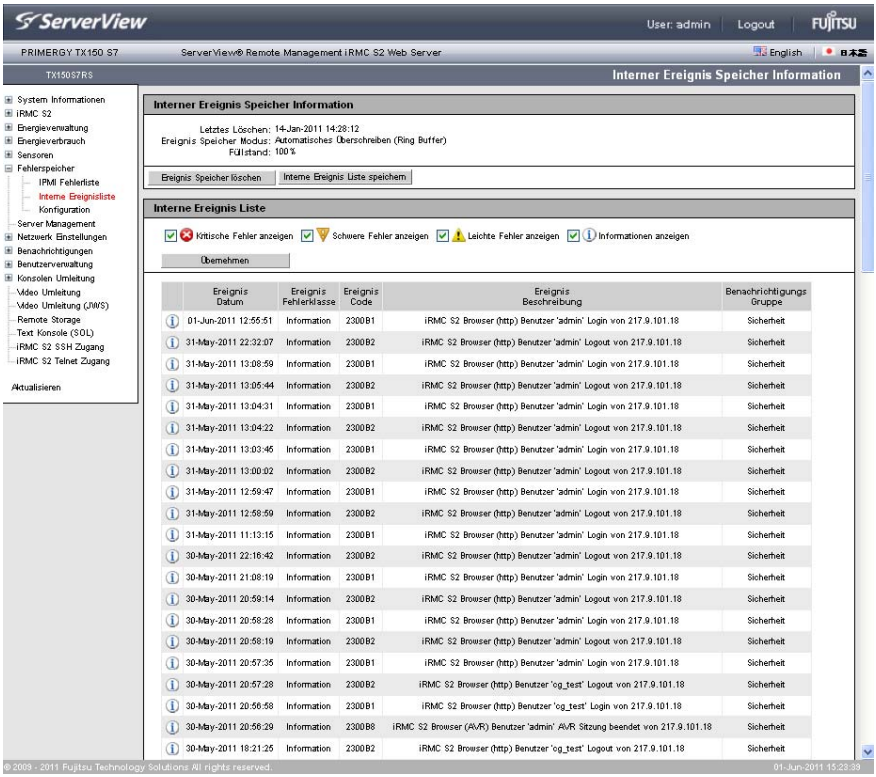

ServerView
User: admin
Logout
FUJITSU
PRIMERGY TX150 S7
ServerView® Remote Management iRMC S2 Web Server
English
TX150S7RS
Interner Ereignis Speicher Information
System Informationen
iRMC S2
Energieverwaltung
Energieverbrauch
Sensoren
Fehlerspeicher
IPMI Fehlerliste
Interne Ereignisliste
Konfiguration
Server Management
Netzwerk Einstellungen
Benachrichtigungen
Benutzerverwaltung
Konsolen Umleitung
Video Umleitung
Video Umleitung (JWS)
Remote Storage
Text Konsole (SOL)
iRMC S2 SSH Zugang
iRMC S2 Telnet Zugang
Aktualisieren
Interner Ereignis Speicher Information
Letztes Löschen: 14-Jan-2011 14:28:12
Ereignis Speicher Modus: Automatisches Überschreiben (Ring Buffer)
Füllstand: 100 %
Ereignis Speicher löschen
Interne Ereignis Liste speichern
Interne Ereignis Liste
Kritische Fehler anzeigen
Schwere Fehler anzeigen
Leichte Fehler anzeigen
Informationen anzeigen
Übernehmen
Ereignis Datum
Ereignis Fehlerklasse
Ereignis Code
Ereignis Beschreibung
Benachrichtigungs Gruppe
01-Jun-2011 12:55:51 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
31-May-2011 22:32:07 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
31-May-2011 13:08:59 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
31-May-2011 13:05:44 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
31-May-2011 13:04:31 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
31-May-2011 13:04:22 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
31-May-2011 13:03:45 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
31-May-2011 13:00:02 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
31-May-2011 12:59:47 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
31-May-2011 12:58:59 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
31-May-2011 11:13:15 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
30-May-2011 22:16:42 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
30-May-2011 21:08:19 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
30-May-2011 20:59:14 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
30-May-2011 20:58:28 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
30-May-2011 20:58:19 Information 2300B2 iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18 Sicherheit
30-May-2011 20:57:35 Information 2300B1 iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18 Sicherheit
30-May-2011 20:57:28 Information 2300B2 iRMC S2 Browser (http) Benutzer 'cg_test' Logout von 217.9.101.18 Sicherheit
30-May-2011 20:56:58 Information 2300B1 iRMC S2 Browser (http) Benutzer 'cg_test' Login von 217.9.101.18 Sicherheit
30-May-2011 20:56:29 Information 2300B8 iRMC S2 Browser (AVR) Benutzer 'admin' AVR Sitzung beendet von 217.9.101.18 Sicherheit
30-May-2011 18:21:25 Information 2300B2 iRMC S2 Browser (http) Benutzer 'cg_test' Logout von 217.9.101.18 Sicherheit
© 2009 - 2011 Fujitsu Technology Solutions All rights reserved.
01-Jun-2011 15:23:39

Bild 127: Seite Interner Ereignis Speicher Information

Interner Ereignis Speicher Information

Die Gruppe *Interer Ereignis Speicher Information* informiert über Füllgrad / die Anzahl der Einträge des internen Ereignisspeichers. Außerdem ist vermerkt, wann zuletzt Einträge hinzugefügt oder gelöscht wurden.

Interner Ereignis Speicher Information
Letztes Löschen: 14-Jan-2011 14:28:12
Ereignis Speicher Modus: Automatisches Überschreiben (Ring Buffer)
Füllstand: 100 %
Ereignis Speicher löschen
Interne Ereignis Liste speichern

Bild 128: Interner Ereignis Speicher Information

Ereignis Speicher löschen

Durch Klicken auf *Ereignis Speicher löschen* löschen Sie alle Einträge im Fehlerspeicher.

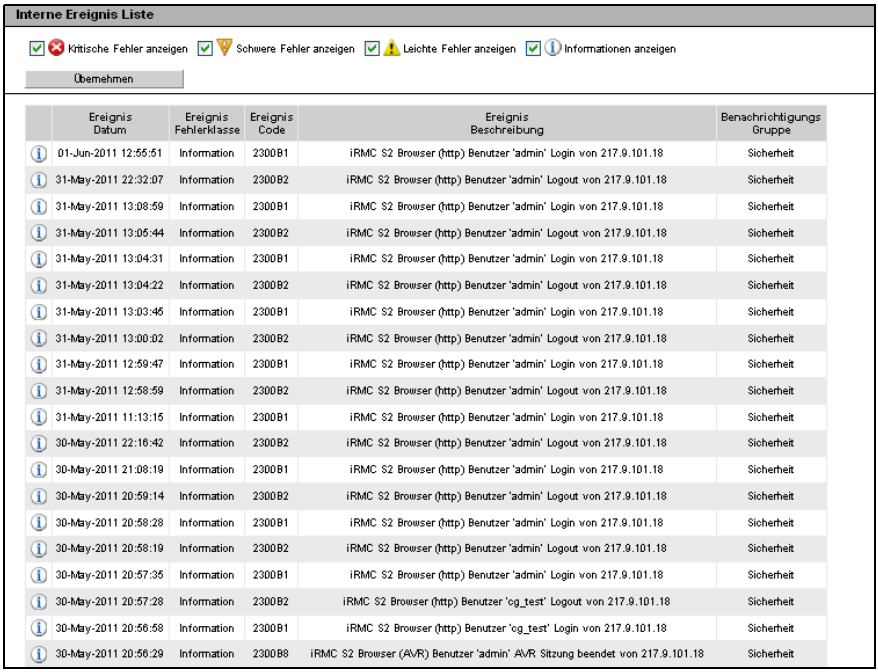
Interne Ereignis Liste speichern

Nach dem Klicken auf *Interne Ereignis Lste speichern* bietet Ihnen der iRMC S2/S3 die Datei *InternalEventLog.sel*, in der die Einträge des internen Ereignisspeichers enthalten sind, zum Herunterladen an.

Interne Ereignisliste

In der Gruppe *Interne Ereignis Liste* werden die Einträge des internen Ereignisspeichers – nach Ereigniskategorien gefiltert – angezeigt.

In der Gruppe *Interne Ereignis Liste* können Sie die Filterkriterien für die Dauer der aktuellen Sitzung modifizieren. Die hier vorgenommenen Einstellungen sind jedoch nur bis zum nächsten Abmelden wirksam. Danach gelten wieder die Standardeinstellungen.



Interne Ereignis Liste

Kritische Fehler anzeigen | Schwere Fehler anzeigen | Leichte Fehler anzeigen | Informationen anzeigen

Übernehmen

Ereignis Datum	Ereignis Fehlerklasse	Ereignis Code	Ereignis Beschreibung	Benachrichtigungs Gruppe
01-Jun-2011 12:55:51	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
31-May-2011 22:32:07	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
31-May-2011 13:08:59	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
31-May-2011 13:05:44	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
31-May-2011 13:04:31	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
31-May-2011 13:04:22	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
31-May-2011 13:03:45	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
31-May-2011 13:00:02	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
31-May-2011 12:59:47	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
31-May-2011 12:58:59	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
31-May-2011 11:13:15	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
30-May-2011 22:16:42	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
30-May-2011 21:08:19	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
30-May-2011 20:59:14	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
30-May-2011 20:58:28	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
30-May-2011 20:58:19	Information	2300B2	iRMC S2 Browser (http) Benutzer 'admin' Logout von 217.9.101.18	Sicherheit
30-May-2011 20:57:35	Information	2300B1	iRMC S2 Browser (http) Benutzer 'admin' Login von 217.9.101.18	Sicherheit
30-May-2011 20:57:28	Information	2300B2	iRMC S2 Browser (http) Benutzer 'cg_test' Logout von 217.9.101.18	Sicherheit
30-May-2011 20:56:58	Information	2300B1	iRMC S2 Browser (http) Benutzer 'cg_test' Login von 217.9.101.18	Sicherheit
30-May-2011 20:56:29	Information	2300B8	iRMC S2 Browser (AVR) Benutzer 'admin' AVR Sitzung beendet von 217.9.101.18	Sicherheit

Bild 129: Seite Interner Ereignis Speicher Information, Interner Ereignis Speicher Liste

Kritische Fehler anzeigen, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*, *Nur CSS Ereignisse anzeigen*

Wählen Sie hier gegebenenfalls ein oder mehrere, von der Standardkonfiguration abweichende Fehlerkategorien aus.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen für die Dauer der aktuellen Sitzung zu aktivieren.

7.10.3 Fehlerspeicher Konfiguration - IPMI SEL und internen Ereignisspeicher konfigurieren

In der Seite *Fehlerspeicher Konfiguration* können Sie den IPMI-Fehlerspeicher und den internen Ereignisspeicher konfigurieren.

Für jeden der beiden Speicher können Sie festlegen

– welche Einträge in der Seite *Fehlerliste* (siehe Seite 230) bzw. in der internen Ereignisliste (siehe Seite 233) standardmäßig angezeigt werden.

– ob der Fehlerspeicher bzw. interne Ereignisspeicher als Ringpuffer oder als linearer Puffer organisiert ist.

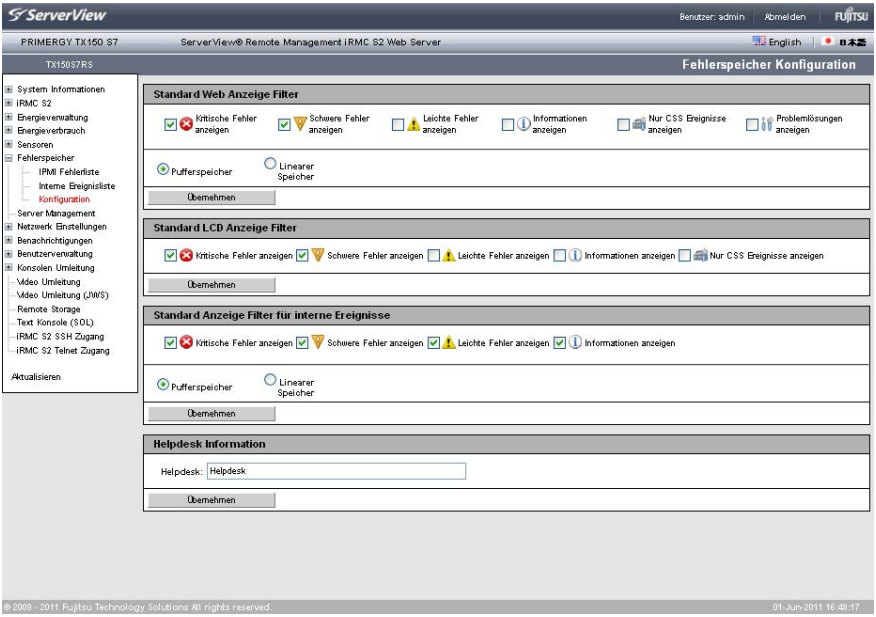


Bild 130: Seite Fehlerspeicher Konfiguration

IPMI-Fehlerspeicher konfigurieren

Standard Web Anzeige Filter

Kritische Fehler anzeigen, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*, *Nur CSS Ereignisse anzeigen*

Wählen Sie hier ein oder mehrere Fehlerkategorien aus, für die in der Seite *Fehlerliste* standardmäßig die Fehlerspeicher-Einträge angezeigt werden sollen.

Problemlösungen anzeigen

Wenn Sie diese Option wählen, wird für jeden Fehlerspeicher-Eintrag der Fehlerkategorie *Kritischer Fehler* oder *Schwerer Fehler* die Ursache und ein Lösungsvorschlag angezeigt.

Pufferspeicher

Der Fehlerspeicher wird als Ringpuffer organisiert.

Linearer Speicher

Der Fehlerspeicher wird als linearer Puffer organisiert.

Wenn der lineare Fehlerspeicher vollständig gefüllt ist, können keine neuen Einträge mehr aufgenommen werden.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Standard LCD Anzeige Filter

Wenn im verwalteten PRIMERGY Server ein ServerView Local Service Display-Modul eingebaut ist, können Sie zusätzlich die Fehlerkategorien für die Anzeige der Fehlerspeicher-Einträge im Anzeigefeld des ServerView Local Service Display-Moduls auswählen. (Diese Auswahl ist unabhängig von der Auswahl, mit der Sie die in der Seite *Fehlerliste* angezeigten Fehlerspeicher-Einträge festlegen.)

Kritische Fehler anzeigen, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*, *Nur CSS Ereignisse anzeigen*

Wählen Sie hier ein oder mehrere Fehlerkategorien aus, für die in der Seite *Fehlerliste* standardmäßig die Fehlerspeicher-Einträge angezeigt werden sollen.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Standard Anzeige Filter für interne Ereignisse

Kritische Fehler anzeigen, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*

Wählen Sie hier ein oder mehrere Fehlerkategorien aus, für die in der Seite *Fehlerliste* standardmäßig die Fehlerspeicher-Einträge angezeigt werden sollen.

Pufferspeicher

Der Ereignisspeicher wird als Ringpuffer organisiert.

Linearer Speicher

Der Ereignisspeicher wird als linearer Puffer organisiert.

Wenn der lineare Ereignisspeicher vollständig gefüllt ist, können keine neuen Einträge mehr aufgenommen werden.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Helpdesk Information

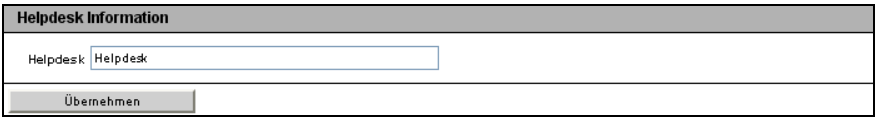


Bild 131: Helpdesk Information

Help desk

String für Helpdesk-Anzeige

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

7.11 Server Management Informationen - Server-Einstellungen konfigurieren

Mithilfe der Seite *Server Management Informationen* können Sie folgende Einstellungen am Server konfigurieren:

– ASR&R-Einstellungen (Automatic Server Reconfiguration and Restart) des Servers (siehe Seite 240)

– Watchdog-Einstellungen (siehe Seite 242)

– Integration von HP System Insight Manager (HP SIM) (siehe Seite 243)

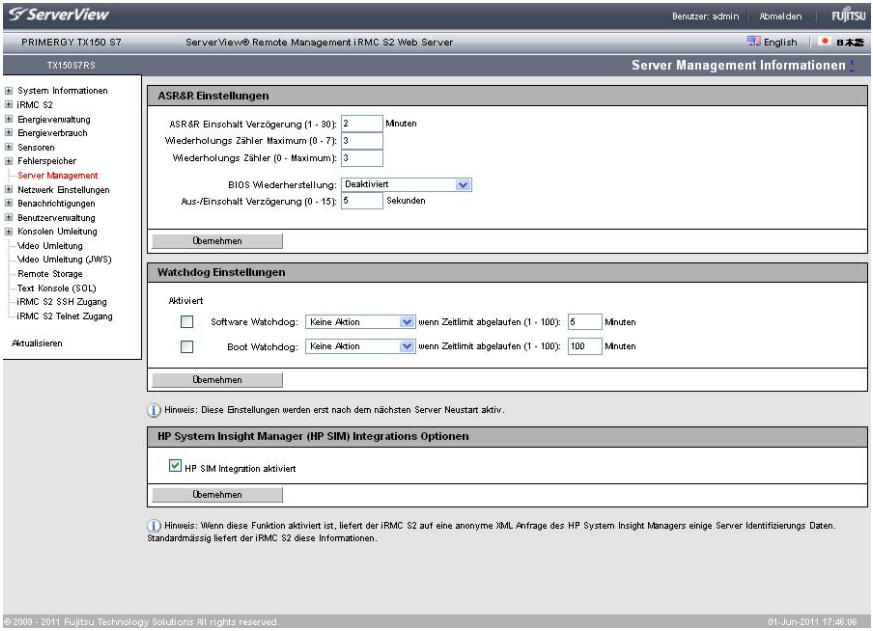


Bild 132: Seite Server Management Informationen

ASR&R Einstellungen - ASR&R-Einstellungen konfigurieren

Mit der Gruppe *ASR&R Einstellungen* konfigurieren sie die ASR&R-Einstellungen (Automatic Server Reconfiguration and Restart) des Servers.

Die Einstellungen der Gruppe *ASR&R Einstellungen* sind erst nach dem nächsten Neustart des Servers wirksam.

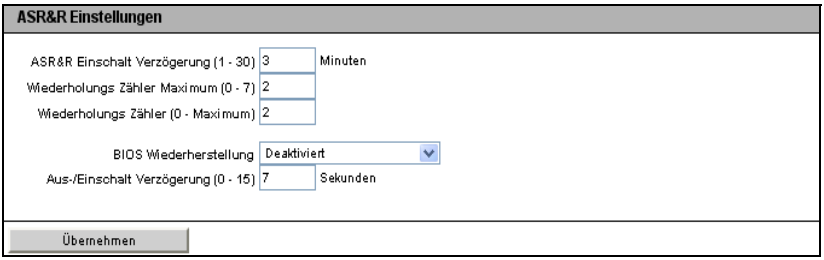


Bild 133: Seite Server Management Informationen - ASR&R Einstellungen

ASR&R Einschalt Verzögerung (1-30)

Anzahl an Minuten (maximal 30 Minuten), die der Server nach einem Aus- und Einschalten aufgrund eines kritischen Fehlers wartet, bevor er einen Neustart-Versuch unternimmt.

Wiederholungs Zähler Maximum (0 - 7)

Maximale Anzahl an Neustart-Versuchen, die für den Server nach einem kritischen Fehler möglich sein soll (maximal 7).

Wiederholungs Zähler (0 - Maximum)

Anzahl an Neustart-Versuchen, die ein Server nach einem kritischen Fehler unternehmen soll (Maximalwert ist der unter *Wiederholungzähler Maximum* eingestellte Wert).

BIOS Wiederherstellung

Das Bit für die BIOS Wiederherstellung (BIOS Recovery Flash Bit) wird aktiviert/deaktiviert:

- *Aktiviert*
  Beim nächsten Starten des Systems wird ein automatischer Flash des BIOS durchgeführt.
- *Deaktiviert*
  Beim nächsten Starten des Systems wird kein automatischer Flash des BIOS durchgeführt.

Die Einstellung *Aktiviert* bietet sich an, wenn nach einer fehlgeschlagenen BIOS-Aktualisierung das Betriebssystem nicht mehr starten kann. Beim nächsten Starten des Systems von der DOS-Diskette (oder einem DOS-Disketten-Image) wird dann das BIOS automatisch wiederhergestellt, d.h. ein BIOS Recovery Flash durchgeführt.

Setzen Sie nach erfolgter BIOS Wiederherstellung die Option *BIOS Wiederherstellung* wieder auf *Deaktiviert*.

Aus-/Einschalt Verzögerung (0 - 15)

Zeitspanne (in Sekunden) zwischen Abschalten und Einschalten während eines automatischen Aus-/Einschalt-Vorgangs (Powercycle).

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu sichern.

Die konfigurierten Einstellungen werden gespeichert und die konfigurierten Aktionen im entsprechenden Fall ausgeführt.

Watchdog Einstellungen - Software Watchdog und Boot Watchdog konfigurieren

Mit der Gruppe *Watchdog Einstellungen* können Sie den Software Watchdog und den Boot Watchdog konfigurieren.

Die Einstellungen der Gruppe *Watchdog Einstellungen* sind erst nach den nächsten Neustart des Servers wirksam.

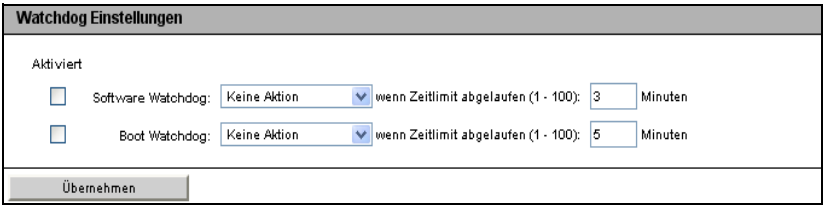


Bild 134: Seite Server Management Informationen - Watchdog Einstellungen

Der **Software Watchdog** überwacht die Arbeit des Systems mithilfe der ServerView-Agenten. Wenn die ServerView-Agenten und das Betriebssystem vollständig initialisiert sind, wird der Software Watchdog aktiviert.
Die ServerView-Agenten kontaktieren in festgelegten Intervallen den iRMC S2/S3. Laufen von einem ServerView-Agenten keine Meldungen mehr ein, wird daraus geschlossen, dass das System nicht mehr ordnungsgemäß läuft.
Für diesen Fall können Sie eine Aktion festlegen.

Der **Boot Watchdog** überwacht die Phase zwischen dem Systemstart und dem Zeitpunkt, zu dem die ServerView-Agenten zur Verfügung stehen.
Wenn die ServerView-Agenten nicht innerhalb eines festgelegten Zeitraums eine Verbindung zum iRMC S2/S3 des Servers aufbauen, wird daraus geschlossen, dass der Startvorgang nicht erfolgreich verlaufen ist.
Für diesen Fall können Sie eine Aktion festlegen.

Gehen Sie wie folgt vor:

- Aktivieren/Deaktivieren Sie unter *Aktiviert* die Option(en) *Software Watchdog* und/oder *Boot Watchdog*.
- Falls Sie ihn aktiviert haben, wählen Sie hinter *Software Watchdog* und/oder hinter *Boot Watchdog* eine folgende Einstellungen:

  Keine Aktion

  Es wird keine Aktion ausgeführt, wenn der Watchdog abgelaufen ist, d.h. der Server läuft weiter. Ein Fehlerspeicher-Eintrag (Eventlog-Eintrag) wird erzeugt.

Neustart
Die Servermanagement-Software löst einen System-Neustart aus.

Aus- und Einschalten
Der Server wird ausgeschaltet und sofort wieder eingeschaltet.

- Geben Sie nach *wenn Zeitlimit abgelaufen (1 - 100)* die Zeitspanne (in Minuten) an, nach deren Verstreichen diese Aktion ausgeführt werden soll.

  Der Boot Watchdog muss solange warten, bis das System gestartet ist. Vereinbaren Sie deshalb für *wenn Zeitlimit abgelaufen (1 - 100)* eine hinreichend große Zeitspanne.

- Klicken Sie auf die Schaltfläche *Übernehmen*.

  Die konfigurierten Einstellungen werden gespeichert und die konfigurierten Aktionen im entsprechenden Fall ausgeführt.

HP System Insight Manager (HP SIM) Integrations Optionen - HP SIM-Integration konfigurieren

Mit der Gruppe *HP System Insight Manager (HP SIM) Integrations Optionen* legen Sie fest, ob der iRMC S2/S3 als Antwort auf eine nicht authentisierte XML-Anfrage des HP Insight Managers Identifizierungsinformationen an diesen zurücksendet.

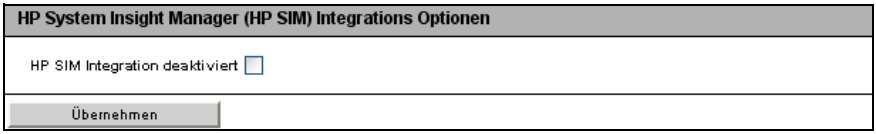


Bild 135: Seite Server Management Informationen - HP SIM Integrations Optionen

Gehen Sie wie folgt vor:

- Aktivieren/deaktivieren Sie die Option *HP SIM Integration deaktiviert*, um die HP SIM-Integration zu deaktivieren bzw. zu aktivieren.
- Klicken Sie auf die Schaltfläche *Übernehmen*, um die gewählte Einstellung zu aktivieren.

7.12 Netzwerk Einstellungen - LAN-Parameter des iRMC S2/S3 konfigurieren

Der Eintrag *Netzwerk Einstellungen* umfasst die Verweise auf die Seiten, mit denen Sie die LAN-Parameter des iRMC S2/S3 konfigurieren:

– "Netzwerk Schnittstelle- Ethernet-Einstellungen des iRMC S2/S3 konfigurieren" auf Seite 245.

– "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 252.

– "DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren" auf Seite 256.

7.12.1 Netzwerk Schnittstelle- Ethernet-Einstellungen des iRMC S2/S3 konfigurieren

Mit der Seite *Netzwerk Schnittstelle* können Sie die Ethernet-Einstellungen des iRMC S2/S3 einsehen und ändern.

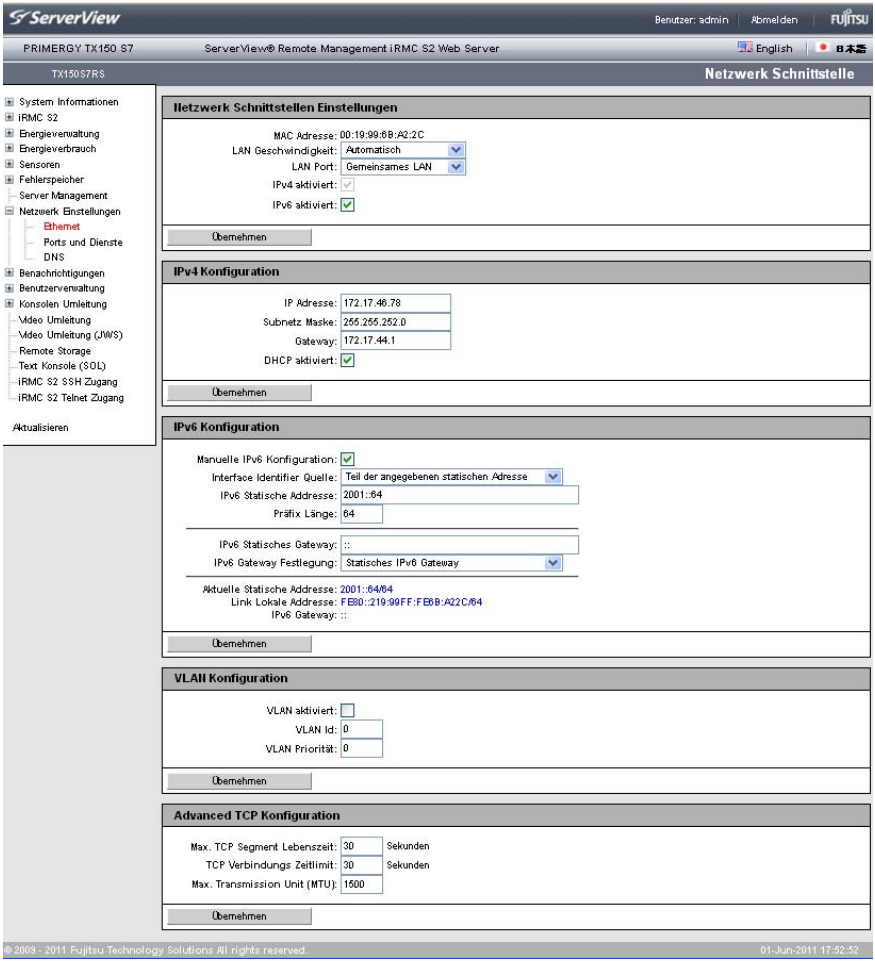


Bild 136: Seite Netzwerk Schnittstelle

ACHTUNG!

Kontaktieren Sie den zuständigen Netz-Administrator, bevor Sie Ethernet-Einstellungen ändern.

Wenn Sie für den iRMC S2/S3 unzulässige Ethernet-Einstellungen konfigurieren, ist ein erneuter Zugriff auf den iRMC S2/S3 nur über eine Konfigurationssoftware, über die serielle Schnittstelle oder im BIOS möglich.

Nur Benutzer mit der Berechtigung *iRMC S2/S3 Einstellungen konfigurieren* können Sie Ethernet-Einstellungen editieren (siehe Kapitel "Benutzerverwaltung für den iRMC S2/S3" auf Seite 69).

Netzwerk Schnittstellen Einstellungen

MAC Adresse

Hier wird die MAC-Adresse des iRMC S2/S3 angezeigt.

LAN Geschwindigkeit

LAN-Geschwindigkeit. Zur Auswahl stehen:

- Automatisch
- 1000 MBit/s Voll Duplex (je nach Server-Hardware)
- 100 MBit/s Voll Duplex
- 100 MBit/s Halb Duplex
- 10 MBit/s Voll Duplex
- 10 MBit/s Halb Duplex

Bei *Automatisch* ermittelt der dem iRMC S2/S3 zugeordnete onboard LAN-Controller selbstständig die korrekte Übertragungsgeschwindigkeit und das Duplex-Verfahren des Netzwerkports, an den er angeschlossen ist.

LAN Port

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

Bei einigen PRIMERGY-Server-Modellen kann die LAN-Schnittstelle der eingebauten System-NIC (Network Interface Card) wahlweise eingerichtet werden als

– *Gemeinsames LAN* für den „Shared“-Betrieb mit dem System oder als

– *Management LAN* exklusiv für das Management LAN.

Für PRIMERGY Server des Typs TX150 S6 ist die Einstellung *Service LAN* zwingend erforderlich.

IPv4 aktiviert

Aktiviert/deaktiviert IPv4-Adressierung für den iRMC S2/S3. Bei aktivierter IPv4-Adressierung wird die Gruppe *IPv4 Konfiguration* angezeigt (siehe unten).

Falls aktuell mit IPv4-Adressierung auf den iRMC S2/S3 zugegriffen wird, können Sie die IPv4-Adressierung nicht deaktivieren.

IPv6 aktiviert

Aktiviert/deaktiviert IPv6-Adressierung für den iRMC S2/S3. Bei aktivierter IPv6-Adressierung wird die Gruppe *IPv6 Konfiguration* angezeigt (siehe unten).

Falls aktuell mit IPv6-Adressierung auf den iRMC S2/S3 zugegriffen wird, können Sie die IPv6-Adressierung nicht deaktivieren.

IPv4 Konfiguration

In der *Gruppe IPv4 Konfiguration* können Sie die IPv4-Einstellungen für den iRMC S2/S3 konfigurieren.

IP Adresse
IPv4-Adresse des iRMC S2/S3 im LAN. Diese Adresse unterscheidet sich von der IP-Adresse des verwalteten Servers.

Falls mit einer statischen Adresse gearbeitet wird (Option *DHCP aktiviert* nicht aktiviert), können Sie diese hier eingeben. Andernfalls (Option *DHCP aktiviert* ist aktiviert) verwendet der iRMC S2/S3 das Feld nur zur Anzeige.

Subnetz Maske
Subnetz-Maske des iRMC S2/S3 im LAN.

Gateway
IP-Adresse des Default-Gateway für das LAN.

DHCP aktiviert
Wenn Sie diese Option aktivieren, erfragt der iRMC S2/S3 seine LAN-Einstellungen von einem DHCP-Server im Netz.

Aktivieren Sie die Option *DHCP* nicht, wenn im Netz kein DHCP-Server verfügbar ist.
Wenn Sie die Option *DHCP* aktivieren und im Netz kein DHCP-Server verfügbar ist, läuft der iRMC S2/S3 in eine Such-Schleife (d.h. er sucht so lange nach einem DHCP-Server, bis er einen findet).

Der (konfigurierte) iRMC S2/S3 kann von einem entsprechend konfigurierten DHCP-Server bei einem DNS-Server registriert werden (siehe Abschnitte "DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren" auf Seite 256).

- Klicken Sie auf *Übernehmen*, um die konfigurierten Einstellungen zu aktivieren.

IPv6 configuration

In der Gruppe *IPv6 Konfiguration* können Sie zusätzlich zur Link-lokalen Adresse „manuell“ eine IPv6-Adresse für den iRMC S2/S3 konfigurieren. Die Link-lokalen Adresse ist dem iRMC S2/S3 immer via „Stateless Autoconfiguration“ zugewiesen ist.

Bei IPv6-Adressierung wird DHCP für den iRMC S2/S3 nicht unterstützt.

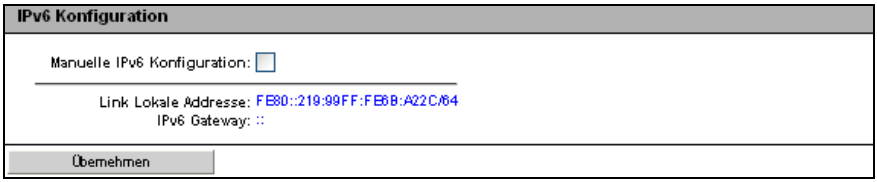


Bild 137: Seite Netzwerk Schnittstelle - Manuelle IPv6 Konfiguration deaktiviert

Manuelle IPv6 Konfiguration

Voreinstellung: deaktiviert.

Wenn Sie die Option *Manuelle IPv6 Konfiguration* aktivieren, zeigt die Gruppe *IPv6 Konfigurierung* zusätzliche Parameter an, mit der Sie manuell eine Routing-fähige IPv6-Adresse für den iRMC S2/S3 konfigurieren können.

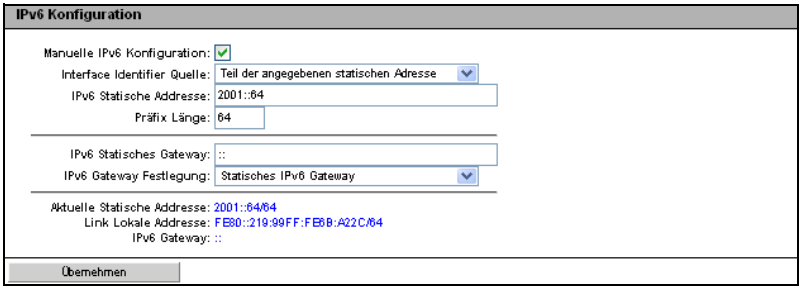


Bild 138: Seite Netzwerk Schnittstelle - Manuelle IPv6 Konfiguration

Interface Identifier Quelle

Spezifiziert die Quelle für den Interface Identifier-Teil der IPv6-Adresse.

Teil der angegebenen statischen Adresse

Teil der statischen IPv6-Adresse, die unter *IPv6 statische Adresse* angegeben ist.

EUI-64 (basierend auf der MAC-Adresse)

EUI-64Standard-konforme Darstellung der MAC-Adresse des iRMC S2/S3.

IPv6 Statische Adresse

Statische IPv6-Adresse für den iRMC S2/S3.

Präfix Länge

Länge des IPv6-Präfix.

IPv6 Statisches Gateway

Statische IPv6-Adresse des Default -Pv6-Gateway im LAN.

IPv6 Gateway Festlegung

IPv6-Gateway, das vom iRMC S2/S3 verwendet wird.

Statisches IPv6 Gateway

Gateway, das unter *IPv6 Statisches Gateway* spezifiziert ist.

Automatisch (vom Router)

Das Gateway wird vom Router automatisch bestimmt.

► Klicken Sie auf *Übernehmen*, um die konfigurierten Einstellungen zu aktivieren.

VLAN Konfiguration

VLAN Id

VLAN-Identifier des virtuellen Netzes (VLAN), dem der iRMC S2/S3 angehört. Zulässiger Wertebereich: 1 ≤ *VLAN Id* ≤ 4094.

VLAN aktiviert

Mithilfe dieser Option aktivieren Sie die VLAN-Unterstützung für den iRMC S2/S3.

VLAN Priorität

VLAN-Priorität (Benutzerpriorität) des iRMC S2/S3 in dem durch *VLAN Id* spezifizierten VLAN.
Zulässiger Wertebereich: 0 ≤ *VLAN Priorität* ≤ 7 (Standardwert: 0).

- Klicken Sie auf *Übernehmen*, um die konfigurierten Einstellungen zu aktivieren.

Advanced TCP Konfiguration

Max. TCP Segment Lebenszeit:

Maximale Lebensdauer (in Sekunden) des TCP/IP-Pakets Voreinstellung: 32 Sekunden).

TCP Verbindungs Zeitlimit

Zeitlimit (in Sekunden) der TCP-Verbindung (Voreinstellung: 32 Sekunden).

Max. Transmission Unit (MTU)

Maximale Paketgröße (in Bytes) der TCP/IP-Datenpakete, die von der TCP/IP-Verbindung akzeptiert werden (Voreinstellung: 3000 Bytes).

- Klicken Sie auf *Übernehmen*, um die konfigurierten Einstellungen zu aktivieren.

7.12.2 Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren

Mit der Seite *Ports und Netzwerk Dienste* können Sie die Konfigurationseinstellungen für die Ports und Netzwerk-Dienste einsehen und ändern.

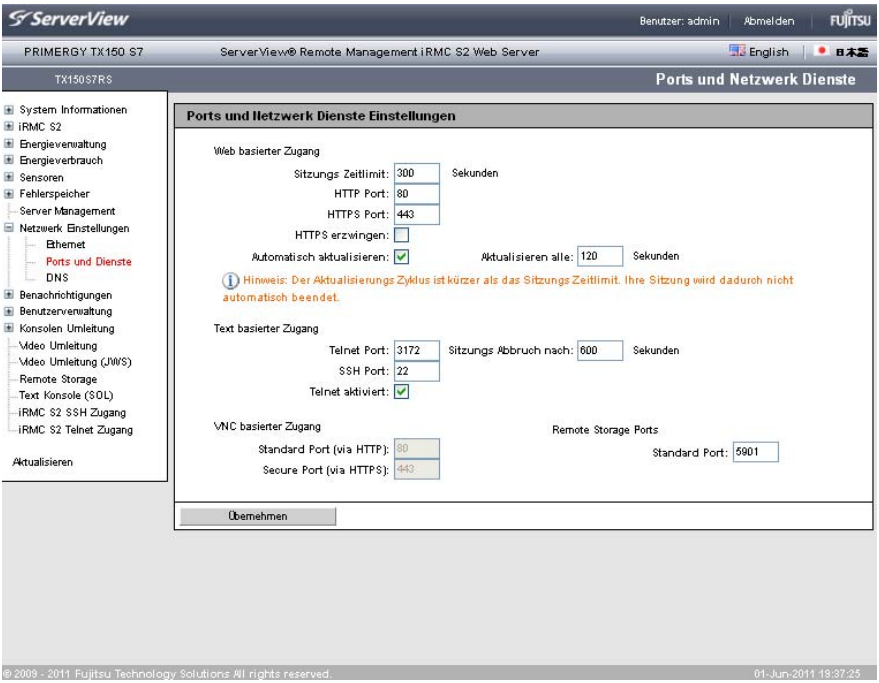


Bild 139: Seite Ports und Netzwerk Dienste

Für Ports, deren Eingabefelder an der iRMC S2/S3-Web-Oberfläche deaktiviert sind, wird eine Konfiguration nicht unterstützt.

Ports für Web-basierten Zugang

Sitzungs Zeitlimit

Zeitspanne (in Sekunden), nach deren Verstreichen Ihre Sitzung bei Inaktivität automatisch beendet wird. Es wird dann die Anmelde-Seite der iRMC S2/S3-Web-Oberfläche angezeigt, über die Sie sich erneut anmelden können (siehe Seite 142).

Ihre Sitzung wird auch bei Inaktivität nicht automatisch nach Ablauf der bei *Sitzungs Zeitlimit* spezifizierten Zeit beendet, wenn Sie bei aktivierter Option *Automatisch aktualisieren* (siehe Seite 254) im Eingabefeld *Aktualisieren alle ... Sekunden* das Aktualisierungsintervall kleiner wählen als den Wert für das *Sitzungs Zeitlimit*.

HTTP Port

HTTP Port des iRMC S2/S3
Standard-Portnummer: 80
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

HTTPS Port

HTTPS (HTTP Secure) Port des iRMC S2/S3
Standard-Portnummer: 443
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

HTTPS erzwingen

Wenn Sie *HTTPS erzwingen* aktivieren, können die Benutzer nur über den im Eingabefeld angegebenen HTTPS-Port eine gesicherte Verbindung zum iRMC S2/S3 aufbauen.

Wenn Sie die Option *HTTPS erzwingen* deaktivieren, können die Benutzer über den im Eingabefeld angegebenen *HTTP Port* eine nicht-gesicherte Verbindung zum iRMC S2/S3 aufbauen.

Wenn das SSL-Zertifikat ausgelaufen ist, wird am Browser eine entsprechende Meldung ausgegeben.

Automatisch aktualisieren

Wenn Sie diese Option aktivieren, wird die Anzeige der iRMC S2/S3-Web-Oberfläche automatisch periodisch aktualisiert. Das Aktualisierungsintervall spezifizieren Sie im Eingabefeld *Aktualisieren alle ... Sekunden*.

Aktualisieren alle ... Sekunden

Länge (in Sekunden) des Intervalls für die automatische Aktualisierung der iRMC S2/S3-Web-Oberfläche.

Wenn Sie das Aktualisierungsintervall kleiner wählen als den Wert für das *Sitzungs Zeitlimit* (siehe Seite 253), wird Ihre Sitzung auch bei Inaktivität nicht automatisch nach Ablauf der bei *Sitzungs Zeitlimit* spezifizierten Zeit beendet.

Ports für Text-basierten Zugang

Telnet Port

Telnet Port des iRMC S2/S3
Standard-Portnummer: 3172
Konfigurierbar: ja
Standardmäßig aktiviert: nein
Kommunikationsrichtung: eingehend und ausgehend

Sitzungs Abbruch nach ... Sekunden

Zeitspanne (in Sekunden), nach deren Verstreichen eine Telnet-Verbindung bei Inaktivität automatisch abgebaut wird.

SSH Port

SSH (Secure Shell) Port des iRMC S2/S3
Standard-Portnummer: 22
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

Telnet aktiviert

Wenn Sie *Telnet aktiviert* aktivieren, können die Benutzer über den im Eingabefeld *Telnet Port* angegebenen Port eine Verbindung zum iRMC S2/S3 aufbauen.

Ports für VNC basierten Zugang

Standard Port (via HTTP)

VNC Port des iRMC S2/S3 für sichere und ungesicherte grafische Konsolen-Umleitung (AVR)
Portnummer: 80
Fest konfiguriert
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend

Secure Port (via HTTPS)

VNC Port des iRMC S2/S3 für die SSL-gesicherte Übertragung von Maus- und Tastatureingaben bei der grafischen Konsolen-Umleitung (AVR).
Portnummer: 443
Fest konfiguriert.
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend

Remote Storage Ports

Standard Port

Standard Remote Storage Port des iRMC S2/S3
Standard-Portnummer: 5901
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

Ab der iRMC S2/S3-Firmware Version 5.00, wird der Remote Storage Port ausschließlich für den Remote Storage Server sowie die Client-interne Kommunikation genutzt. Für die integrierte Remote Storage-Funktionalität (Remote Storage-Verbindung via AVR), wird der HTTP-Port 80 verwendet.

- Klicken Sie auf *Übernehmen*, um die konfigurierten Einstellungen zu aktivieren.

7.12.3 DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren

Mit der Seite *DNS Konfiguration* können Sie für den iRMC S2/S3 den Domain Name Service (DNS) aktivieren und einen Hostnamen für den iRMC S2/S3 konfigurieren.

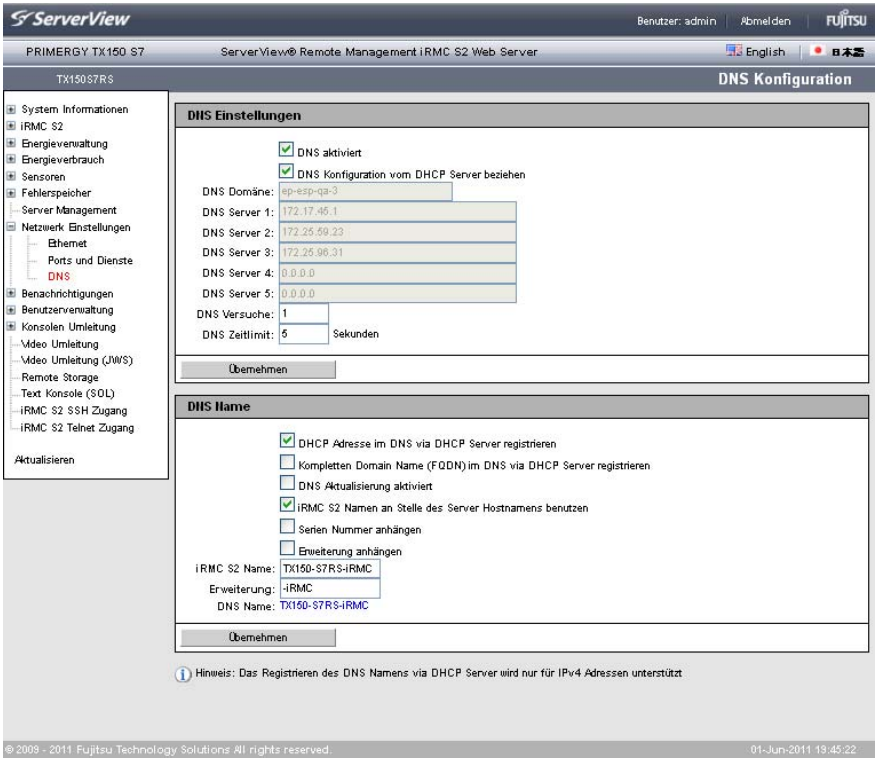


Bild 140: Seite DNS Konfiguration

DNS Einstellungen

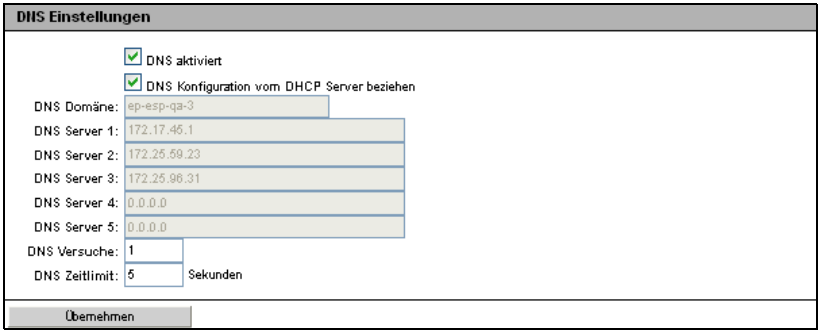


Bild 141: Seite DNS Konfiguration - DNS Einstellungen

DNS aktiviert

Aktiviert / deaktiviert DNS für den iRMC S2/S3.

DNS Konfiguration vom DHCP Server beziehen

Wenn Sie diese Option aktivieren, werden die IP-Adressen der DNS-Server automatisch vom DHCP-Server übernommen.
In diesem Fall werden bis zu fünf DNS-Server unterstützt.

Wenn Sie diese Einstellung nicht aktivieren, können Sie unter *DNS-Server 1* - *DNS-Server 5* bis zu fünf DNS-Serveradressen manuell eingeben.

DNS Domäne

Wenn die Option *DNS Konfiguration vom DHCP Server beziehen* deaktiviert ist, geben Sie hier den Namen der Default-Domäne für Anfragen an den bzw. die DNS Server an.

DNS Server 1 .. 5

Wenn die Option *DNS Konfiguration vom DHCP Server beziehen* deaktiviert ist, können Sie hier die IP-Adressen von bis zu fünf der DNS-Servern angeben.

DNS Versuche

Anzahl der DNS-Retries.

DNS Zeitlimit

Zeitlimit (in Sekunden) für eine Antwort des DNS.

- Klicken Sie auf die *Übernehmen*, um die konfigurierten Einstellungen zu speichern.

DNS Name

In der Gruppe *DNS Name* können Sie einen Hostnamen für den iRMC S2/S3 konfigurieren und so “dynamic DNS” nutzen. Mit „Dynamic DNS“ können DHCP-Server die IP-Adresse und den Systemname einer Netzkomponente selbstständig zur besseren Identifikation an DNS-Server weitergeben.

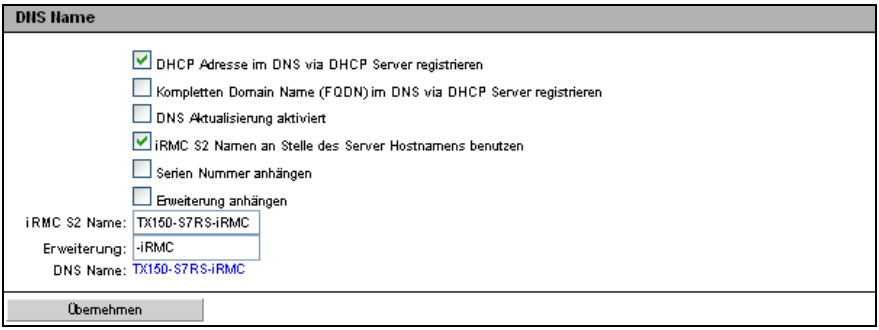

DNS Name
DHCP Adresse im DNS via DHCP Server registrieren
Kompletten Domain Name (FQDN) im DNS via DHCP Server registrieren
DNS Aktualisierung aktiviert
iRMC S2 Namen an Stelle des Server Hostnamens benutzen
Serien Nummer anhängen
Erweiterung anhängen
iRMC S2 Name: TX150-S7RS-iRMC
Erweiterung: -iRMC
DNS Name: TX150-S7RS-iRMC
Übernehmen

Bild 142: Seite DNS Konfiguration - DNS Name

DHCP Adresse im DNS via DHCP Server registrieren

Wenn IPv6-Adressierung verwendet wird, ist diese Option deaktiviert. Aktiviert / deaktiviert für den iRMC S2/S3 die DHCP-Namensübergabe an den DHCP Server sowie die DNS Registrierung via DHCP Server.

Kompletten Domain Name (FQDN) im DNS via DHCP Server registrieren

Wenn IPv6-Adressierung verwendet wird, ist diese Option deaktiviert. Aktiviert / deaktiviert für den iRMC S2/S3 die Übergabe des FQDN (Fully Qualified Domain Name) an den DHCP Server sowie die DNS Registrierung via DHCP Server.

DNS Aktualisierung aktiviert

Aktiviert / deaktiviert die Aktualisierung von DNS Records via Dynamic DNS.

iRMC S2/S3 Namen an Stelle des Server Hostnamens benutzen

Der im Dialogfeld *iRMC S2/S3 Name* spezifizierte iRMC S2/S3-Name wird anstelle des Servernamens verwendet.

Serien Nummer anhängen

Dem DHCP-Namen für den iRMC S2/S3 werden rechts die letzten 3 Bytes der MAC-Adresse des iRMCS2/S3 hinzugefügt.

Erweiterung anhängen

Dem DHCP-Namen für den iRMC S2/S3 wird die im Dialogfeld *Erweiterung* eingetragene Erweiterung hinzugefügt.

iRMC S2/S3 Name

iRMC S2/S3-Name, der für den iRMC S2/S3 anstelle des Servernamens an DHCP weitergegeben wird. Abhängig von den entsprechenden Optionen wird der iRMC S2/S3-Name als Bestandteil des DNS-Namens verwendet.

Erweiterung

Namenserweiterung für den iRMC S2/S3.

DNS Name

Zeigt den konfigurierten DNS-Namen für den iRMC S2/S3.

► Klicken Sie auf die *Übernehmen*, um die konfigurierten Einstellungen zu speichern.

7.13 Benachrichtigungen - Alarmbenachrichtigung konfigurieren

Der Eintrag *Benachrichtigungen* enthält die Verweise auf die Seiten, mit denen Sie die Alarmbenachrichtigung (Alerting) konfigurieren können:

– "SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren" auf Seite 261.

– "Serielle / Modem Benachrichtigungen - Alarmweiterleitung über Modem konfigurieren" auf Seite 263.

– "E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren" auf Seite 265.

7.13.1 SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren

In der Seite *SNMP Trap Benachrichtigung* können Sie die Einstellungen der SNMP Trap-Benachrichtigung (SNMP-Alarmweiterleitung) einsehen und konfigurieren.

Es wird die Weiterleitung von SNMP-Traps an bis zu sieben SNMP-Server unterstützt.

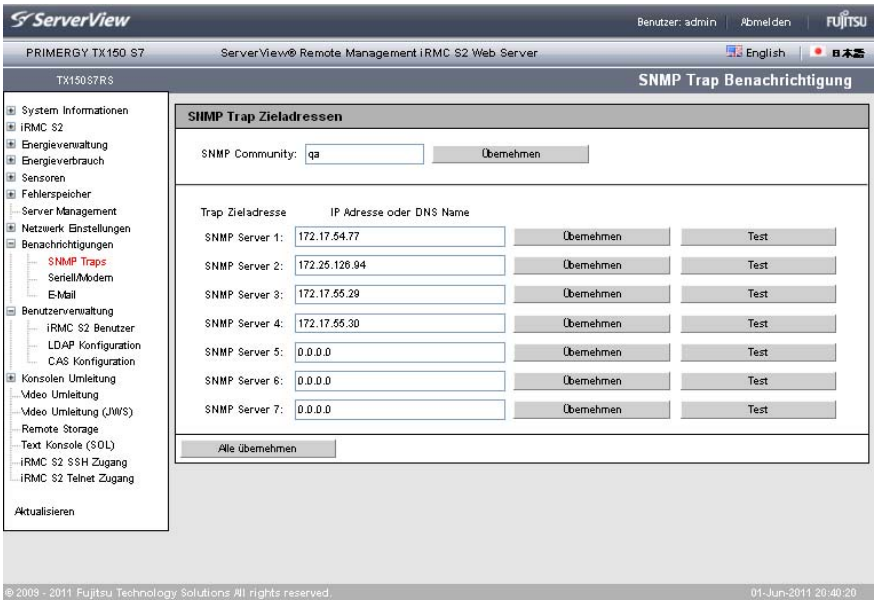


Bild 143: Seite SNMP Trap Benachrichtigung

SNMP Community

Name der SNMP-Community.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um den Community-Namen zu übernehmen.

SNMP Server1 .. SNMP Server7 (Trap-Zieladressen)
DNS-Namen oder IP-Adressen der Server, die dieser SNMP-Community angehören und als Trap-Ziele konfiguriert werden sollen.

- ► Klicken Sie auf die Schaltfläche *Übernehmen*, um den SNMP Server als Trap-Ziel zu aktivieren.
- ► Klicken Sie auf die Schaltfläche *Test*, um die Verbindung zum SNMP Server zu testen.

► Klicken Sie gegebenenfalls auf *Alle übernehmen*, um alle Einstellungen zu aktivieren.

7.13.2 Serielle / Modem Benachrichtigungen - Alarmweiterleitung über Modem konfigurieren

Die Seite *Serielle / Modem Benachrichtigungen* wird nur in Verbindung mit dem iRMC S2 angezeigt.

Mithilfe der Seite *Serielle / Modem Benachrichtigungen* konfigurieren Sie die Weiterleitung von Alarmen über Modem.

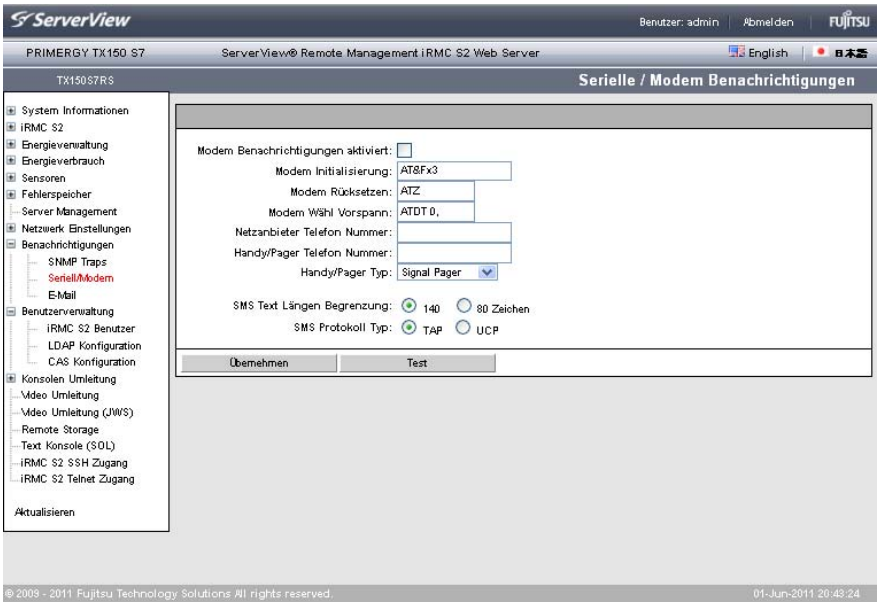


Bild 144: Seite Serielle / Modem Benachrichtigungen

Modem Benachrichtigungen aktiviert

Benachrichtigungen via Modem werden aktiviert /deaktiviert.

Modem Initialisierung

Entnehmen Sie diese Eingabe der Dokumentation zu Ihrem Modem.

Modem Rücksetzen

Entnehmen Sie diese Eingabe der Dokumentation zu Ihrem Modem.

Modem Wähl Vorspann

Diese Eingabe ist abhängig von der Art des Anschlusses.

Netzanbieter Telefon Nummer

Geben Sie die Nummer des SMS-Servers an.

Handy/Pager Telefon Nummer

Geben Sie die Nummer des Mobiltelefons an.

Handy/Pager Typ

Hier können Sie wählen zwischen:

- Signal Pager
- Numeric Pager
- Alpha Pager
- SMS
- DoCoMo

SMS Text Längen Begrenzung

Als maximale Länge können Sie wahlweise die Werte 80 oder 140 einstellen.

SMS Protokoll Typ

Aktivieren Sie die Option, die für das genutzte Mobilfunk-Netz steht.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Klicken Sie auf die Schaltfläche *Test*, um eine Test-Benachrichtigung zu senden.

7.13.3 E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren

Mithilfe der Seite *E-Mail Benachrichtigung* konfigurieren Sie die Einstellungen für die E-Mail-Benachrichtigung an lokale Benutzerkennungen.

Es wird die Konfiguration von zwei Mail Servern unterstützt.

E-Mail-Benachrichtigung kann für jeden Benutzer individuell festgelegt werden (siehe Abschnitt "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 275).

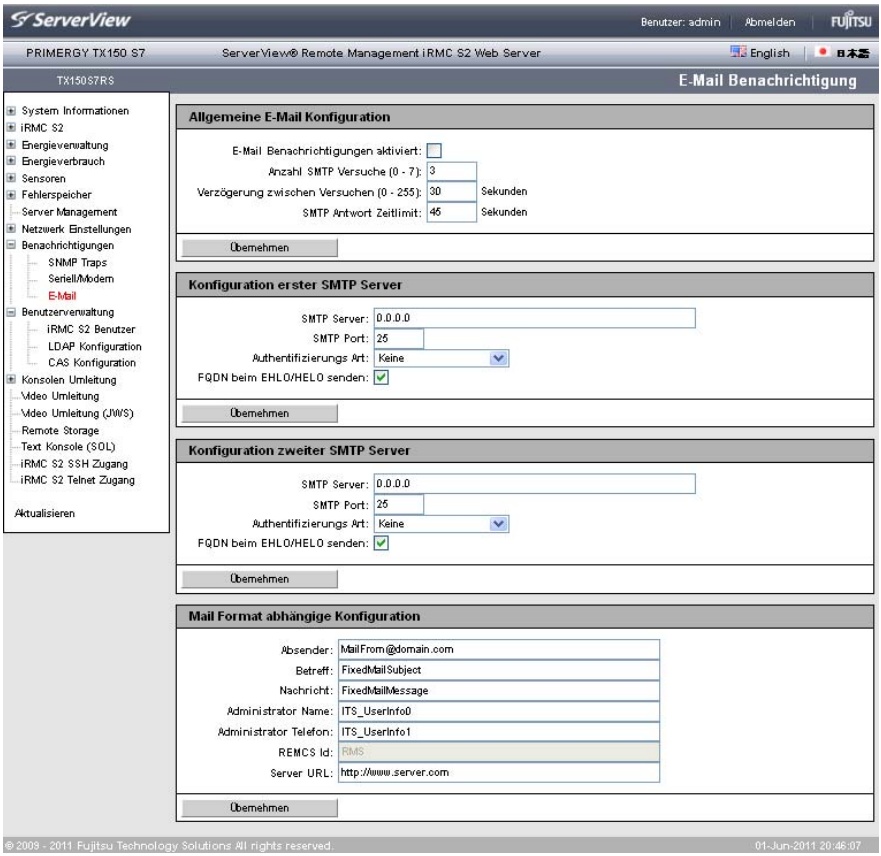


Bild 145: Seite E-Mail Benachrichtigung

Allgemeine E-Mail Konfiguration- Allgemeine E-Mail-Einstellungen konfigurieren

Mit der Gruppe *Allgemeine E-Mail Konfiguration* konfigurieren Sie die allgemeinen E-Mail-Einstellungen.

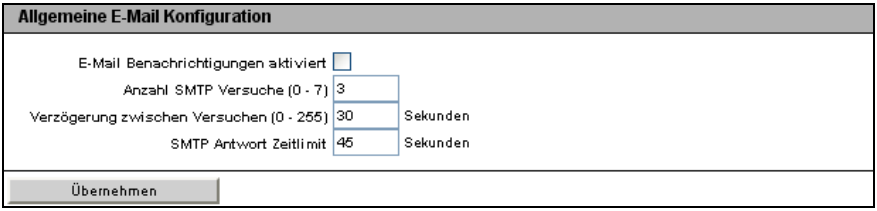


Bild 146: Seite E-Mail Benachrichtigung - Allgemeine E-Mail Konfiguration

E-Mail Benachrichtigungen aktiviert
Aktivieren Sie diese Option.

SMTP Anzahl Versuche (0 - 7)
Anzahl möglicher SMTP-Versuche.

Verzögerungen zwischen Versuchen (0 - 255)
Zeitspanne (in Sekunden) zwischen den einzelnen SMTP-Versuchen.

SMTP Antwort Zeitlimit
Zeitlimit (in Sekunden) für SMTP-Antwort.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Konfiguration erster SMTP Server - Ersten Mail Server konfigurieren

Mit der Gruppe *Konfiguration erster SMTP Server* konfigurieren Sie den ersten (primären) Mail Server (SMTP Server).

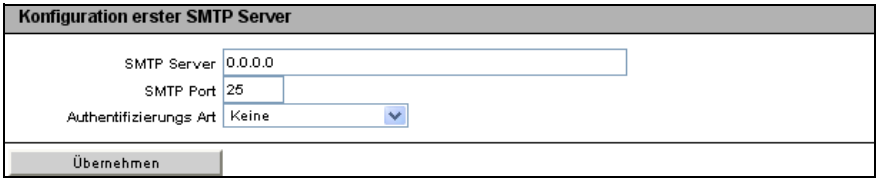


Bild 147: Seite E-Mail Benachrichtigung - Konfiguration erster SMTP Server

SMTP Server

IP-Adresse des primären Mail Servers.

> Sie können für den iRMC S2/S3 den Domain Name Service (DNS) aktivieren (siehe "DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren" auf Seite 256). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

SMTP Port

SMTP Port des Mail Servers

Authentifizierungs Art

Art der Authentifizierung einer Verbindung des iRMC S2/S3 zum Mail Server:

- *Keine*
  Keinerlei Authentifizierung der Verbindung.
- *SMTP AUTH (RFC 2554)*
  Authentifizierung nach RFC 2554: SMTP Service Extension for Authentication.
  In diesem Fall werden folgende Eingaben erwartet:

  Auth. Benutzer Name
  Benutzername für die Authentisierung beim Mail Server

  Auth. Kennwort
  Kennwort für die Authentisierung beim Mail Server

  Kennwort bestätigen
  Bestätigen Sie hier Ihr Kennwort.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Konfiguration zweiter SMTP Server - Zweiten Mail Server konfigurieren

Mit der Gruppe *Konfiguration zweiter SMTP Server* konfigurieren Sie den zweiten (sekundären) Mail Server (SMTP Server).

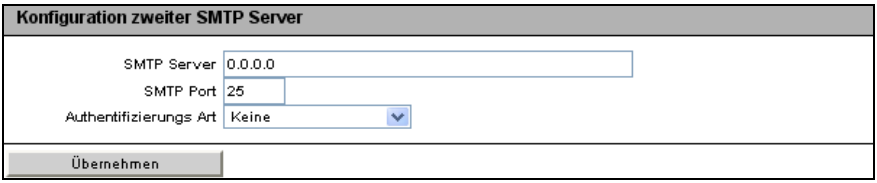


Bild 148: Seite E-Mail Benachrichtigung - Konfiguration zweiter SMTP Server

SMTP Server
IP-Adresse des sekundären Mail Servers.

Sie können für den iRMC S2/S3 den Domain Name Service (DNS) aktivieren (siehe "DNS Konfiguration - DNS für den iRMC S2/S3 konfigurieren" auf Seite 256). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

SMTP Port
SMTP Port des Mail Servers

Auth Type
Einstellung für die Authentifizierung einer Verbindung des iRMC zum Mail Server:

- *None*
  Keinerlei Authentifizierung der Verbindung.
- *SMTP AUTH (RFC 2554)*
  Authentifizierung nach RFC 2554: SMTP Service Extension for Authentication

Auth User Name
Benutzername für die Authentisierung beim Mail Server

Auth Password
Passwort für die Authentisierung beim Mail Server

Confirm Password
Bestätigen Sie hier Ihr Passwort.

Authentifizierungs Art
Art der Authentifizierung einer Verbindung des iRMC S2/S3 zum Mail Server:

– *Keine*
  Keinerlei Authentifizierung der Verbindung.

– *SMTP AUTH (RFC 2554)*
  Authentifizierung nach RFC 2554: SMTP Service Extension for Authentication.
  In diesem Fall werden folgende Eingaben erwartet:

  Auth. Benutzer Name
  Benutzername für die Authentisierung beim Mail Server

  Auth. Kennwort
  Kennwort für die Authentisierung beim Mail Server

  Kennwort bestätigen
  Bestätigen Sie hier Ihr Kennwort.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Mail Format abhängige Konfiguration - Mail-Format-abhängige Einstellungen konfigurieren

Mit der Gruppe *Mail Format abhängige Konfiguration* konfigurieren Sie die vom Mail-Format abhängigen Einstellungen. Das Mail-Format konfigurieren Sie Benutzer-spezifisch auf der Seite *Benutzer '<Name>' Konfiguration* (Gruppe *E-Mail Konfiguration*, siehe Seite 279).

Es werden die folgenden Mail-Formate unterstützt:

- Standard
- Fixed Subject
- ITS-Format
- Fujitsu REMCS Format

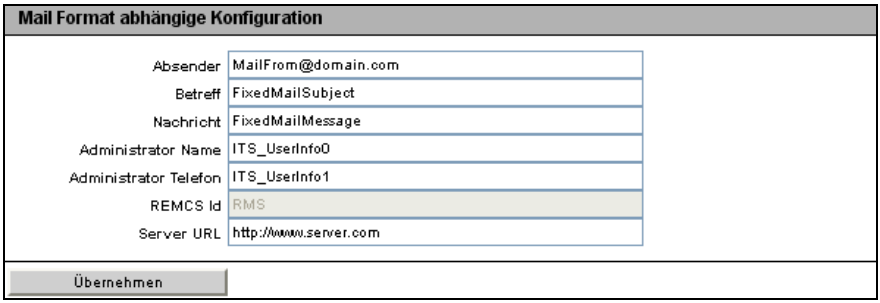


Bild 149: Seite E-Mail Benachrichtigung - Mail Format abhängige Konfiguration

Je nach Mail-Format sind nicht alle Eingabefelder aktiv.

Absender

Identifikation des sendenden iRMC S2/S3.
Aktiv bei allen Mail-Formaten.

> **i** Wenn in der hier eingegebenen Zeichenfolge ein „@“ enthalten ist, wird diese Zeichenfolge als gültige E-Mail-Adresse interpretiert. Andernfalls wird „admin@<ip-adresse>“ als gültige E-Mail-Adresse verwendet.

Betreff

Betreff der Alarmmeldung-E-Mails.
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 279).

Nachricht

Art der Mitteilung (E-Mail).
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 279).

Administrator Name

Name des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 279).

Administrator Telefon

Telefonnummer des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 279).

REMCS Id

Diese ID ist eine zusätzliche Indentifikation des Servers, ähnlich der Seriennummer.
Aktiv nur bei Mail-Format *Fujitsu REMCS-Format*.

Server URL

Eine URL, unter der der Server unter bestimmten Voraussetzungen zugänglich ist. Sie müssen die URL manuell eingeben.
Aktiv nur bei Mail-Format *Standard*.

► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu speichern.

7.14 Benutzerverwaltung

Der Eintrag *Benutzerverwaltung* enthält die Verweise auf die Seiten für die lokale Benutzerverwaltung sowie für die Konfiguration des Verzeichnisdienstes (Directory Service) zur globalen Benutzerverwaltung (LDAP-Konfiguration):

- "Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S2/S3" auf Seite 272
- "Verzeichnisdienst Konfiguration (LDAP) - Verzeichnisdienst am iRMC S2/S3 konfigurieren" auf Seite 282
- "Centralized Authentication Service (CAS) Konfiguration - CAS Service konfigurieren" auf Seite 296

7.14.1 Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S2/S3

Die Seite *Benutzer Verwaltung* enthält eine tabellarische Übersicht über alle konfigurierten Benutzer: Pro Zeile werden die Daten eines konfigurierten Benutzers dargestellt. Die Benutzernamen sind dabei als Verweise realisiert. Durch Klicken auf einen Benutzernamen öffnet sich das Fenster *Benutzer '<name>' Konfiguration* (siehe Seite 275), in dem Sie die Einstellungen des betreffenden Benutzers einsehen und/oder modifizieren können.

Die Benutzer Id 1 („Null-User“) ist reserviert für den IPMI-Standard und steht deshalb nicht für die Benutzerverwaltung am iRMC S2/S3 zur Verfügung.

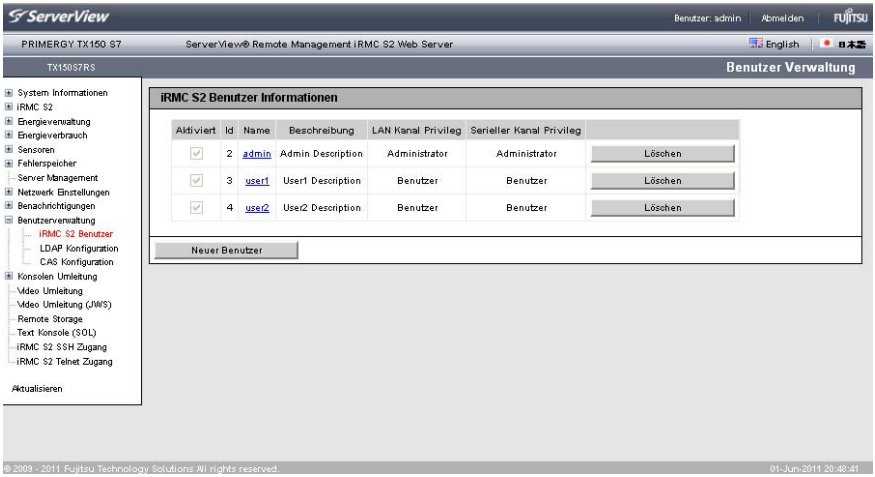


Bild 150: Seite Benutzer Verwaltung

Löschen

In der Tabelle der konfigurierten Benutzer finden Sie hinter jedem Benutzereintrag eine Schaltfläche *Löschen*. Durch Klicken auf diese Schaltfläche können Sie den zugehörigen Benutzer nach nochmaliger Bestätigung löschen.

Neuer Benutzer

Wenn Sie auf diese Schaltfläche klicken, öffnet sich die Seite *Neuen Benutzer konfigurieren* (siehe Seite 274), über die Sie einen neuen Benutzer konfigurieren können.

7.14.1.1 Neuen Benutzer konfigurieren

Mithilfe der Seite *Neuen Benutzer konfigurieren* konfigurieren Sie die Grundeinstellungen eines neuen Benutzers.

Erläuterungen zu den Feldern und Auswahllisten der Seite *Neuen Benutzer konfigurieren* finden Sie ab Seite 276 bei der Beschreibung der Seite *Benutzer '<Name>' Konfiguration*.

In Bild 151 ist die Konfiguration eines Benutzers „User3“ dargestellt.

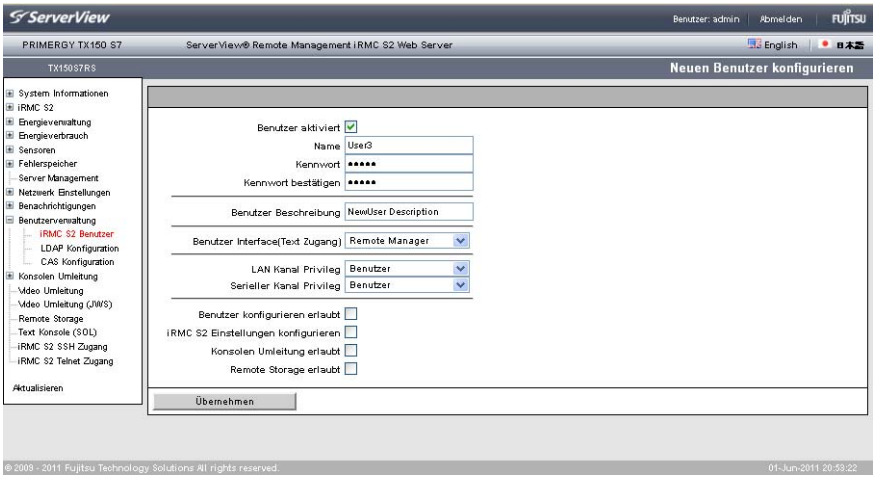


Bild 151: Seite Benutzer Verwaltung - Neuen Benutzer konfigurieren

7.14.1.2 Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)

Mithilfe der Seite *Benutzer '<name>' Konfiguration* können Sie die Einstellungen für einen Benutzer einsehen, ändern und erweitern.

In Bild 152 ist die Konfiguration des in Bild 151 neu angelegten Benutzers *user3* dargestellt.

Die Benutzer Id wird, in Klammern eingeschlossen, hinter dem Benutzernamen angezeigt.

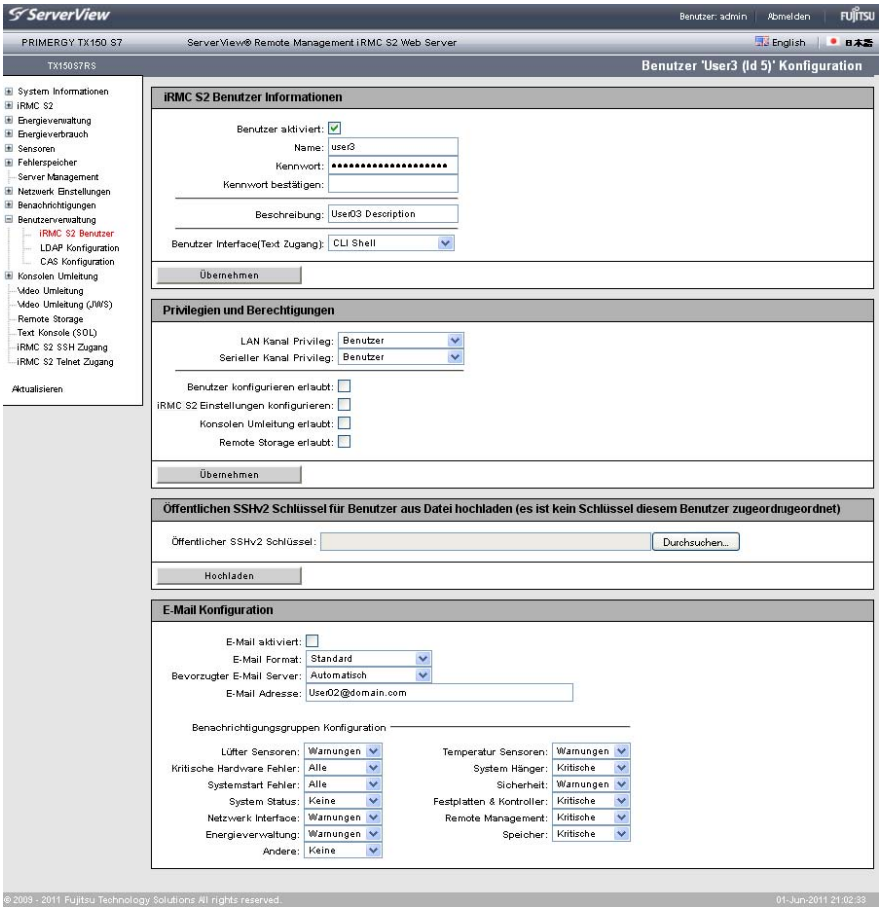


Bild 152: Seite Benutzer Verwaltung - Benutzer '<name>' Konfiguration

iRMC S2/S3 Benutzer Informationen - Zugangsdaten des Benutzers konfigurieren

Mit der Gruppe *iRMC S2/S3 Benutzer Informationen* konfigurieren Sie die Zugangsdaten des Benutzers.

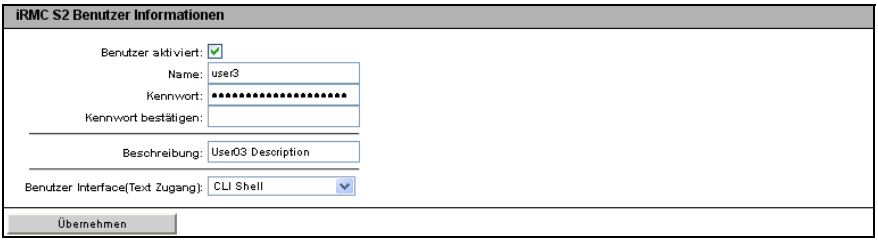


Bild 153: Benutzer '<name>' Konfiguration - iRMC S2/S3 Benutzer Informationen

Benutzer aktiviert
Durch Deaktivieren dieser Option können Sie den Benutzer sperren.

Name
Tragen Sie hier den Namen des Benutzers ein.

Kennwort
Tragen Sie hier das Kennwort des Benutzers ein.

Kennwort bestätigen
Wiederholen Sie hier zur Bestätigung die Eingabe des Kennworts.

Beschreibung
Tragen Sie hier eine allgemeine Beschreibung des konfigurierten Benutzers ein.

Benutzer Interface (Text Zugang)
Wählen Sie hier die gewünschte Text-basierte Benutzerschnittstelle aus. Zur Auswahl stehen:

- *SMASH CLP*
  Siehe Abschnitt "Start a Command Line shell... - SMASH CLP Shell starten" auf Seite 351.
- *Remote Manager*
  Siehe Kapitel "iRMC S2/S3 über Telnet/SSH (Remote Manager)" auf Seite 333.

- *IPMI Terminal Mode*
- *None*

► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

Privilegien und Berechtigungen - Benutzerprivilegien und Benutzerberechtigungen konfigurieren

Mit der Gruppe *Privilegien und Berechtigungen* konfigurieren Sie die Kanal-spezifischen Benutzerprivilegien sowie die Kanal-unabhängigen Berechtigungen.

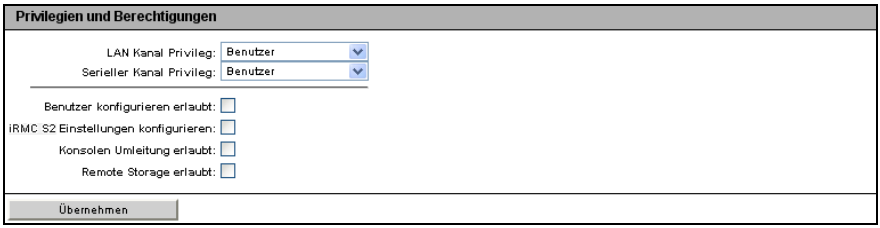


Bild 154: Benutzer '<name>' Konfiguration - Privilegien und Berechtigungen

LAN Kanal Privileg

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den LAN-Kanal zu:

- *Benutzer*
- *Operator*
- *Administrator*
- *OEM*

Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt "Benutzerberechtigungen" auf Seite 72.

Serieller Kanal Privileg

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den seriellen Kanal zu. Zur Auswahl stehen die gleichen Berechtigungsgruppen wie unter *LAN Kanal Privileg*.

Ergänzend zu den Kanal-spezifischen Privilegien können Sie einem Benutzer individuell folgende Kanal-unabhängigen Berechtigungen erteilen:

Benutzer konfigurieren erlaubt
: Berechtigung zum Konfigurieren von lokalen Benutzerzugangsdaten.

iRMC S2/S3 Einstellungen konfigurieren
: Berechtigung zum Konfigurieren der iRMC S2/S3-Einstellungen.

Konsolen Umleitung erlaubt
: Berechtigung zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection, AVR) im „Nur Lesen“- und „Volle Kontrolle“-Modus.

Remote Storage erlaubt
: Berechtigung zur Nutzung der Remote Storage-Funktionalität.

- Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen

Mit der Gruppe *Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen* können Sie für den zu konfigurierenden Benutzer einen öffentlichen SSHv2-Schlüssel aus einer Datei hochladen.

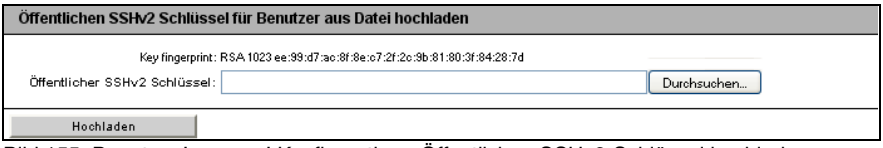


Bild 155: Benutzer '<name>' Konfiguration - Öffentlichen SSHv2-Schlüssel hochladen

Näheres zur SSHv2 Public Key-Authentisierung für lokale Benutzer finden Sie im Abschnitt "SSHv2 Public Key-Authentifizierung für lokale iRMC S2/S3-Benutzer" auf Seite 76.

E-Mail Konfiguration - Benutzer-spezifische E-Mail-Einstellungen konfigurieren

Mit der Gruppe *E-Mail Konfiguration* konfigurieren Sie die Benutzer-spezifischen Einstellungen für das E-Mail-Format.

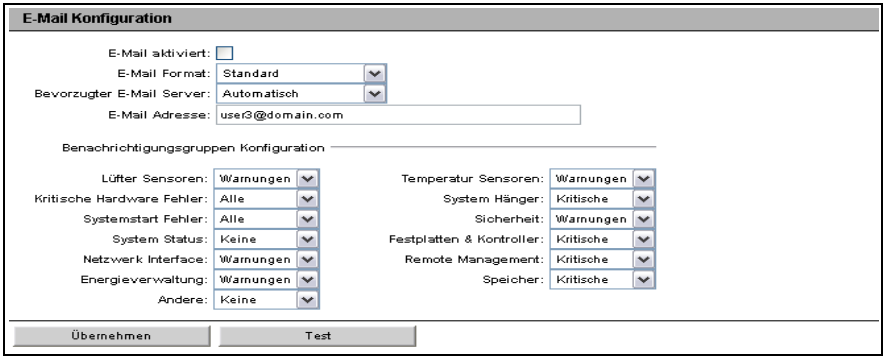


Bild 156: Benutzer '<name>' Konfiguration - E-Mail Konfiguration

E-Mail aktiviert

Hier stellen Sie ein, ob der Benutzer per E-Mail über die Systemzustände informiert werden soll.

E-Mail Format

Abhängig vom gewählten Mail-Format können Sie in der Seite *E-Mail Benachrichtigung* (Gruppe Mail Format dependent Configuration, siehe Seite 270) unterschiedliche Einstellungen vornehmen.

Folgende Mail-Formate stehen zur Verfügung:

- *Standard*
- *Fester Betreff*
- *ITS-Format*
- *Fujitsu REMCS Format*

Bevorzugter E-Mail Server

Bevorzugter Mail Server.
Sie können zwischen folgenden Optionen wählen:

– *Automatisch*

  Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z. B. der erste Mail-Server nicht verfügbar ist, wird E-Mail an den zweiten Mail-Server gesendet.

– *Erster*

  Nur der als *Erster SMTP Server* (siehe Seite 267) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

– *Zweiter*

  Nur der als *Zweiter SMTP Server* (siehe Seite 268) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

Fehler beim Versenden der E-Mail erzeugen einen Eintrag im Fehlerspeicher.

E-Mail Adresse

E-Mail-Adresse des Empfängers.

Benachrichtigungsgruppen Konfiguration

Hier können Sie Systemereignisse konfigurieren, über die ein iRMC S2/S3-Benutzer per E-Mail benachrichtigt werden soll.

Jeder Eintrag im Fehlerspeicher (Eventlog-Eintrag) des iRMC S2/S3 wird einer bestimmten Benachrichtigungsgruppe zugeordnet.

Für jede Benachrichtigungsgruppe sind folgende Einstellungen möglich:

Keine

Die Benachrichtigungsfunktion für diese Benachrichtigungsgruppe ist deaktiviert.

Kritische

Der iRMC S2/S3 benachrichtigt den Benutzer per E-Mail, wenn ein Fehlerspeicher-Eintrag die Ereignisklasse *Kritisch* meldet.

Warnungen

Der iRMC S2/S3 benachrichtigt den Benutzer per E-Mail, wenn ein Fehlerspeicher-Eintrag ein Ereignis der Klassen *Leichte Fehler*, *Schwere Fehler* oder *Kritische Fehler* meldet.

Alle

Der iRMC S2/S3 benachrichtigt den Benutzer über jedes zu einem Eintrag in den Fehlerspeicher führende Ereignis in dieser Benachrichtigungsgruppe.

► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

7.14.2 Verzeichnisdienst Konfiguration (LDAP) - Verzeichnisdienst am iRMC S2/S3 konfigurieren

Für die globale Benutzerverwaltung über einen Verzeichnisdienst (Directory Service) müssen Sie den iRMC S2/S3 mithilfe der Seite *Verzeichnisdienst Konfiguration* entsprechend konfigurieren.

Derzeit werden LDAP-Zugriffe des iRMC S2/S3 für die Verzeichnisdienste Microsoft Active Directory, Novell eDirectory und OpenLDAP unterstützt.

Die folgenden Zeichen sind in LDAP als Meta-Zeichen für Such-Strings reserviert: *, \, &, (,), |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

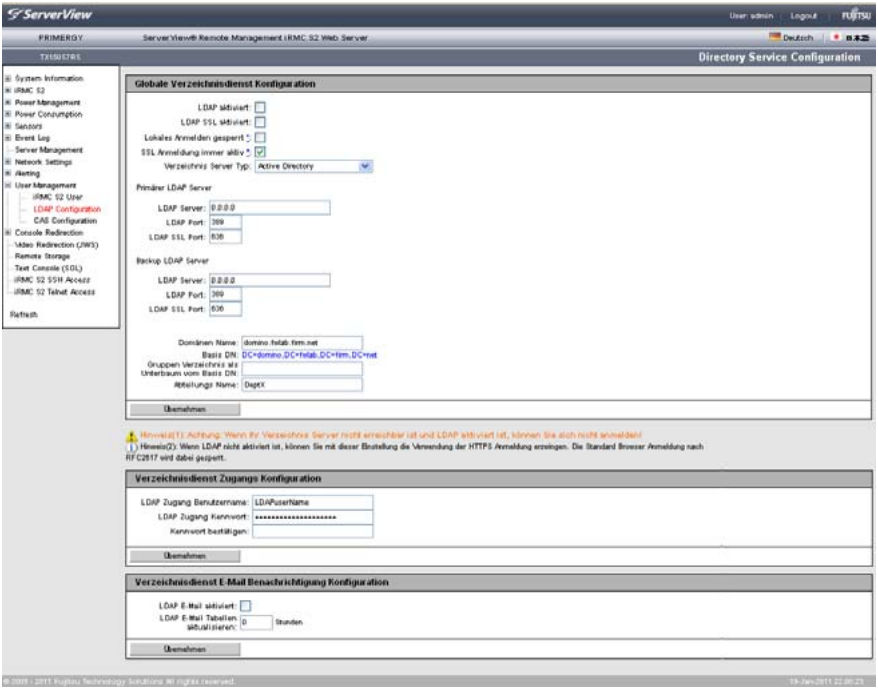


Bild 157: Seite Verzeichnisdienst Konfiguration (LDAP-Konfiguration)

LDAP aktiviert

Mit dieser Option legen Sie fest, ob der iRMC S2/S3 via LDAP auf einen Verzeichnisdienst zugreifen kann. Der Verzeichnisdienst via LDAP kann nur genutzt werden, wenn *LDAP aktiviert* aktiviert ist.

Wenn *LDAP aktiviert* aktiviert ist, wird die Anmelde-Information (siehe Seite 142) immer SSL-verschlüsselt zwischen dem Web-Browser und dem iRMC S2/S3 übertragen.

LDAP SSL aktiviert

Wenn Sie diese Option aktivieren, erfolgt der Datenaustausch zwischen iRMC S2/S3 und Verzeichnisserver (Directory Server) SSL-verschlüsselt.

LDAP SSL aktiviert hat keinen Einfluss darauf, ob die Seiten der iRMC S2/S3-Web-Oberfläche SSL-gesichert geöffnet werden oder nicht.

LDAP SSL aktiviert sollten Sie nur aktivieren, wenn ein Domänencontroller-Zertifikat (Domain Controller-Zertifikat) installiert ist.

Lokales Anmelden gesperrt

Wenn Sie diese Option aktivieren, werden alle iRMC S2/S3-lokalen Benutzerkennungen gesperrt, und nur die durch den Verzeichnisdienst verwalteten Benutzkennungen sind gültig.

ACHTUNG!

Wenn die Option *Lokales Anmelden gesperrt* aktiviert ist und außerdem die Verbindung zum Verzeichnisdienst fehlschlägt, ist am iRMC S2/S3 kein Anmelden mehr möglich.

SSL Anmeldung immer aktiv

Diese Option ist nur relevant, wenn gleichzeitig LDAP deaktiviert ist.

Wenn Sie diese Option aktivieren, wird stets die HTTP SSL-gesicherte Anmelde-Seite verwendet, auch wenn LDAP deaktiviert ist. Nur wenn Sie *SSL Anmeldung immer aktiv* nicht aktivieren und außerdem LDAP deaktiviert ist, kommt eine über Digest Authentication Login gesicherte Maske zum Einsatz.

Verzeichnis Server Typ

Typ des verwendeten Verzeichnisservers.

Folgende Verzeichnisdienste werden unterstützt:

- *Active Directory*: Microsoft Active Directory
- *Novell*: Novell eDirectory
- *OpenLDAP*: OpenLDAP

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Je nach gewähltem Verzeichnisdienst werden unterschiedliche Eingabefelder angeboten:

- Zu *Active Directory* siehe "iRMC S2/S3 für Microsoft Active Directory konfigurieren" auf Seite 285.
- Zu *eDirectory* und *OpenLDAP* siehe "iRMC S2/S3 für Novell eDirectory / OpenLDAP / OpenDS konfigurieren" auf Seite 290.

7.14.2.1 iRMC S2/S3 für Microsoft Active Directory konfigurieren

Nachdem Sie Ihre Wahl *Active Directory* mit *Übernehmen* bestätigt haben, wird die folgende Variante der Seite *Verzeichnisdienst Konfiguration* angezeigt:

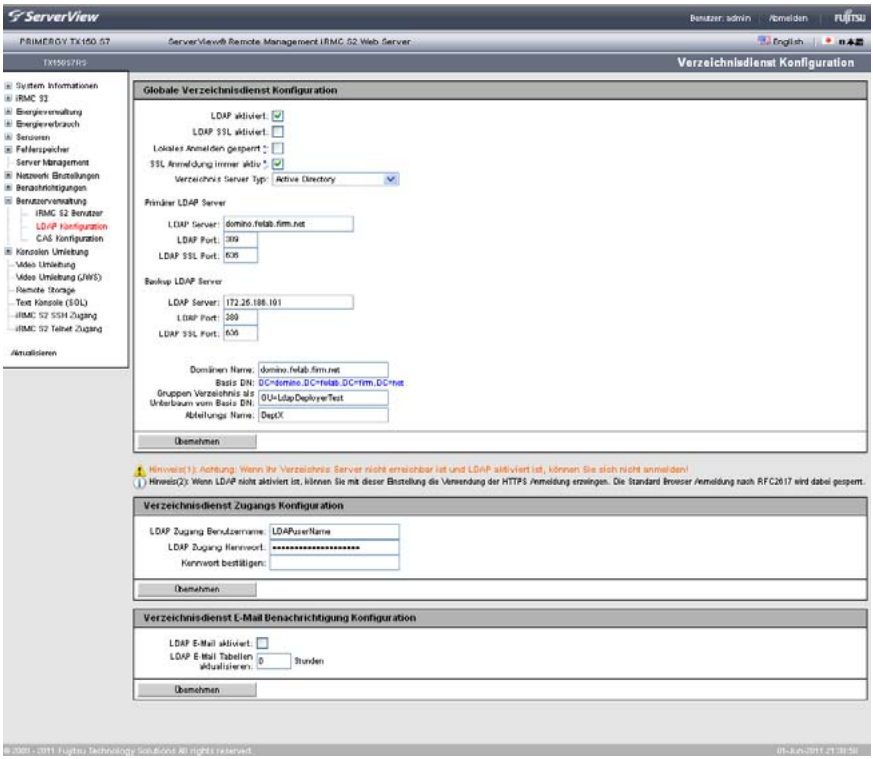


Bild 158: Verzeichnisdienst Konfiguration: Angaben für Microsoft Active Directory

Gehen Sie wie folgt vor:

► Vervollständigen Sie Ihre Angaben Sie in der Gruppe *Globale Verzeichnisdienst Konfiguation*:

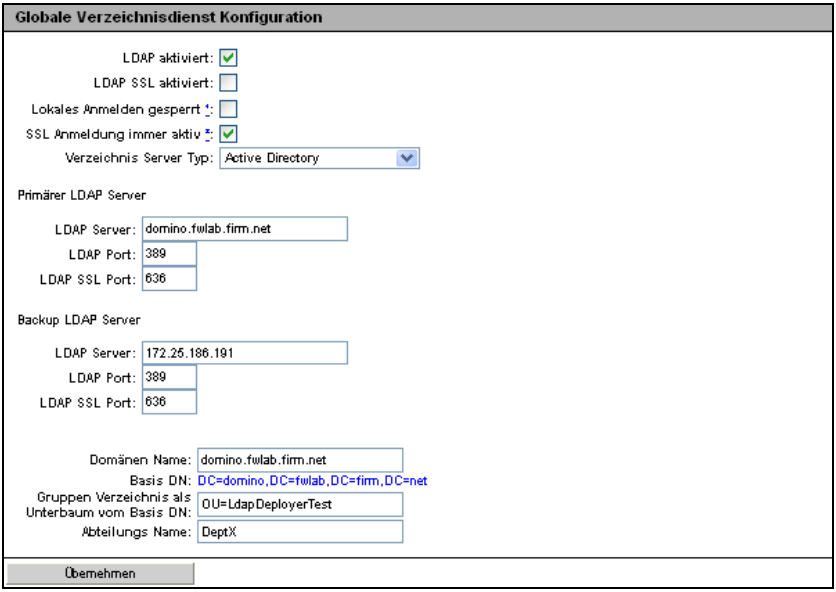


Bild 159: Globale Verzeichnisdienst Konfiguration: Angaben für Microsoft Active Directory

Primärer LDAP Server

LDAP Verzeichnisserver, der verwendet werden soll.

LDAP Server

IP-Adresse oder DNS-Name des primären Verzeichnisservers.

LDAP Port

LDAP-Port des primären Verzeichnisservers.

LDAP SSL Port

Sicherer LDAP-Port des primären Verzeichnisservers.

Backup LDAP Server

LDAP Verzeichnisserver, der als Backup-Server geführt und bei Ausfall des primären LDAP Servers als Verzeichnisserver herangezogen wird.

LDAP Server
IP-Adresse oder DNS-Name des Backup LDAP Verzeichnisservers.

LDAP Port
LDAP-Port des Backup LDAP Verzeichnisservers.

LDAP SSL Port
Sicherer LDAP-Port des Backup LDAP Verzeichnisservers.

Domänen Name
Vollständiger DNS-Pfadname des Verzeichnisservers.

Basis DN
Basis DN wird automatisch von *Domänen Name* abgeleitet.

Gruppen Verzeichnis als Unterbaum vom Basis DN
Pfadname der Organisationseinheit (OU) der als Teilbaum des *Basis DN* (Group DN Context) die OUs *SVS* oder *iRMCgroups* enthält.

Abteilungs Name
Der Abteilungsname wird im Verzeichnisdienst zur Bestimmung der Benutzerrechte und Benachrichtigungsgruppen (Alert Roles) benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen in zu aktivieren.

► Konfigurieren Sie den LDAP-Zugang in der Gruppe *Verzeichnisdienst Zugangs Konfiguation*:

Die hier vorzunehmenden Einstellungen werden für die Alarm-Benachrichtigung (Alerting) im Zusammenhang mit globalen Benutzerkennungen benötigt. Falls die Alarmbenachrichtigung nicht aktiviert ist, sind die Einstellungen der Gruppe *Verzeichnisdienst Zugangs Konfiguation* nicht relevant.

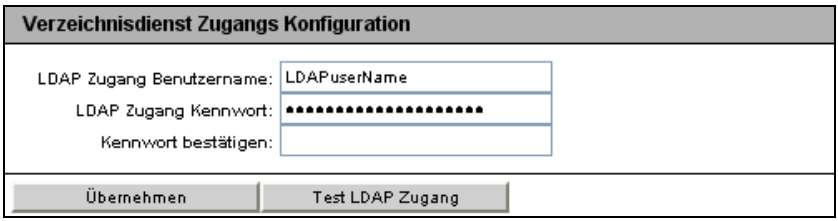


Bild 160: Microsoft Active Directory: Verzeichnisdienst Zugangs Konfiguration

LDAP Zugang Benutzername

Benutzername, unter dem sich der iRMC S2/S3 beim LDAP-Server anmeldet.

LDAP Zugang Kennwort

Kennwort, mit dem sich der Benutzername beim LDAP-Server authentisiert.

Kennwort bestätigen

Wiederholen Sie das unter *LDAP Zugang Kennwort* eingegebene Kennwort.

Test LDAP Zugang

Überprüft die Zugangsdaten zum LDAP-Verzeichnisserver und zeigt als Ergebnis den LDAP-Status an (siehe Bild 161).

Dieser Test prüft lediglich die Basis-Zugangsdaten („LDAP-Server vorhanden?“, „Benutzer konfiguriert?“), führt jedoch keine vollständige Autorisierung des Benutzers durch.

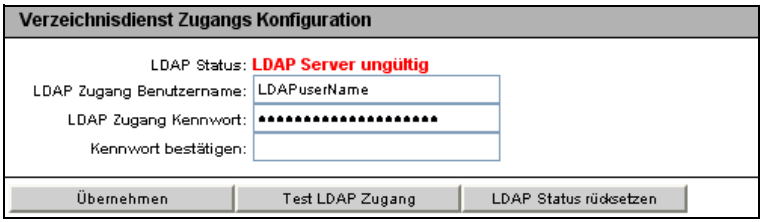


Bild 161: Microsoft Active Directory: Status der Verbindung zum LDAP-Server

► Klicken Sie auf *LDAP Status zurücksetzen*, um die Statusanzeige zurückzusetzen.

► Klicken Sie auf *Übernehmen,* um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie in der Gruppe *Verzeichnisdienst E-Mail Benachrichtigung Konfiguration* die Einstellungen für globale E-Mail-Benachrichtigung.

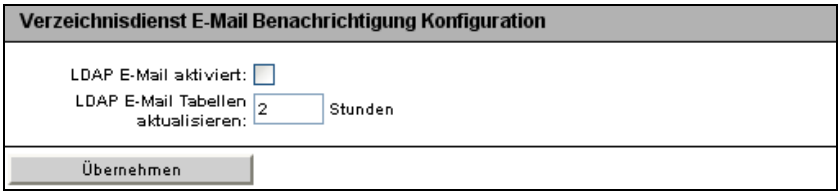


Bild 162: Verzeichnisdienst E-Mail Benachrichtigung Konfiguration

LDAP E-Mail aktiviert
Aktiviert die globale E-Mail-Benachrichtigung.

LDAP E-Mail Tabellen aktualisieren [Stunden]
Definiert das Intervall für die regelmäßige Aktualisierung der E-Mail-Tabelle. Der Wert „0“ bedeutet: keine regelmäßige Aktualisierung.

Es wird dringend empfohlen, einen Wert >0 anzugeben. Der Wert “0” hat zur Folge, dass die Tabelle nicht regelmäßig aktualisiert wird.

► Klicken Sie auf *Übernehmen,* um Ihre Einstellungen zu aktivieren.

7.14.2.2 iRMC S2/S3 für Novell eDirectory / OpenLDAP / OpenDS konfigurieren

Nachdem Sie Ihre Wahl *Novell* oder *OpenLDAP* mit *Übernehmen* bestätigt haben, wird die nachfolgend beschriebene Variante der Seite *Verzeichnisdienst Konfiguration* angezeigt.

Der Aufbau der Seite *Verzeichnisdienst Konfiguration* ist für Novell eDirectory und OpenLDAP identisch.

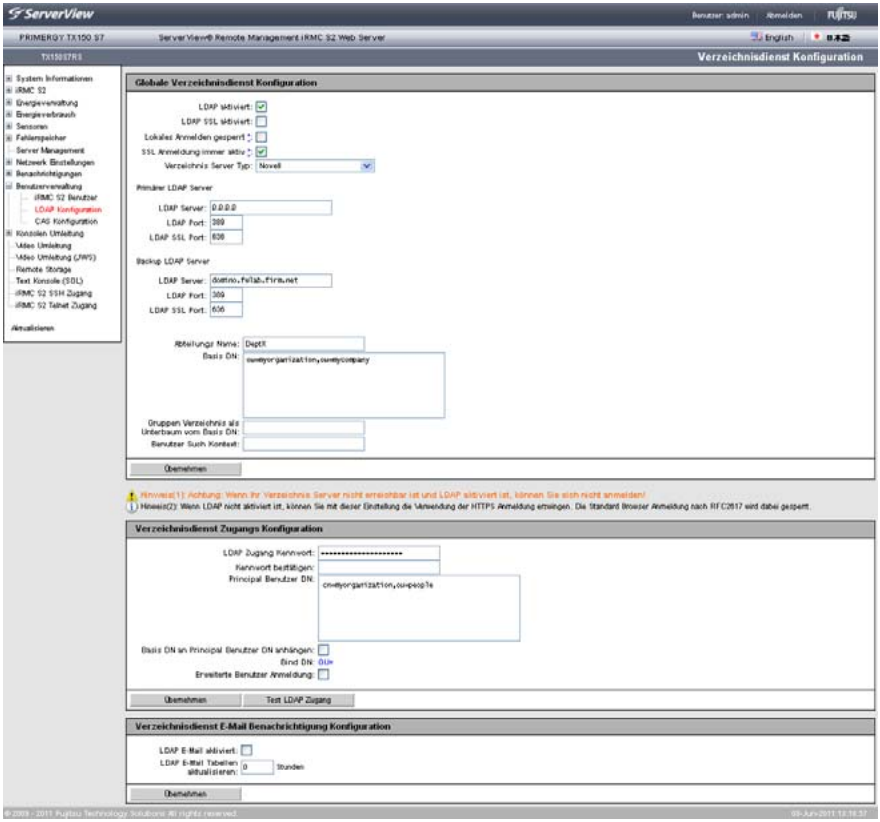


Bild 163: Globale Verzeichnisdienst Konfiguration: Angaben für Novell eDirectory / OpenLDAP/ OpenDS

Gehen Sie wie folgt vor:

► Vervollständigen Sie Ihre Angaben Sie in der Gruppe *Globale Verzeichnisdienst Konfiguation:*

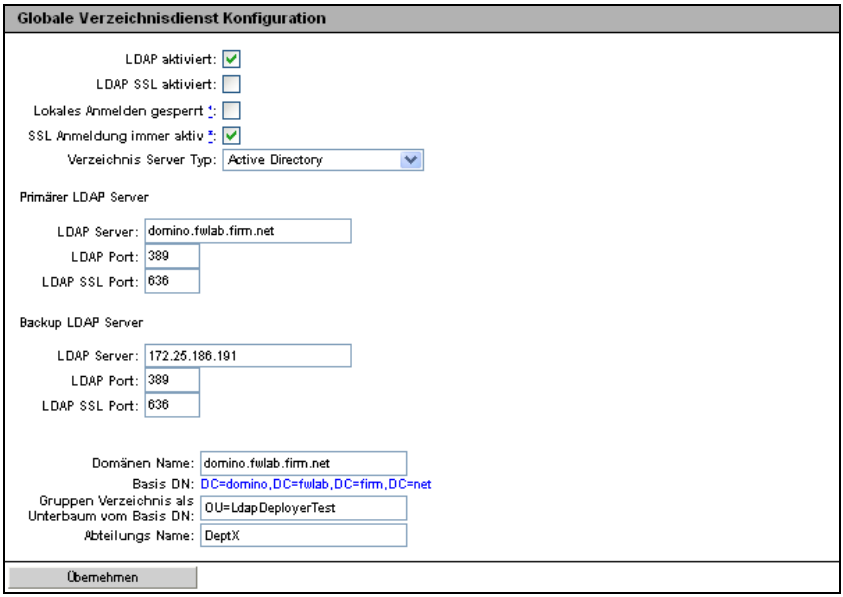


Bild 164: Novell eDirectory / OpenLDAP / OpenDS: Globale Verzeichnisdienst Konfiguration

Primärer LDAP Server

LDAP Verzeichnisserver, der verwendet werden soll.

LDAP Server

IP-Adresse oder DNS-Name des primären Verzeichnisservers.

LDAP Port

LDAP-Port des primären Verzeichnisservers.

LDAP SSL Port

Sicherer LDAP-Port des primären Verzeichnisservers.

Backup LDAP Server

LDAP Verzeichnisserver, der als Backup-Server geführt und bei Ausfall des primären LDAP Servers als Verzeichnisserver herangezogen wird.

LDAP Server

IP-Adresse oder DNS-Name des Backup LDAP Verzeichnisservers.

LDAP Port

LDAP-Port des Backup LDAP Verzeichnisservers.

LDAP SSL Port

Sicherer LDAP-Port des Backup LDAP Verzeichnisservers.

Abteilungs Name

Abteilungsname. Der Abteilungsname wird im Verzeichnisdienst zur Bestimmung der Benutzerrechte benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y.

Basis DN

Der *Basis DN* (Base DN) ist der „vollständig eindeutige Name“ (Fully Distinguished Name) des eDirectory OpenLDAP OpenDS Servers und repräsentiert den Baum oder Teilbaum, in dem die Organisationseinheit (Organizational Unit, OU) *SVS* oder *iRMCgroups* enthalten ist. Dieser DN bildet den Ausgangspunkt für LDAP-Suchoperationen.

Gruppen Verzeichnis als Unterbaum vom Basis DN

Pfadname der Organisationseinheit, die als Teilbaum von *Base DN* (Group DN Context) die Organisationseinheiten *SVS* oder *iRMCgroups* enthält).

Benutzer Such Kontext

Pfadname der Organisationseinheit, die als Teilbaum von *Base DN* (User Search Context) die Organisationseinheit *Users* enthält.

► Klicken Sie auf *Übernehmen,* um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie den LDAP-Zugang in der Gruppe *Verzeichnisdienst Zugangs Konfiguation*:

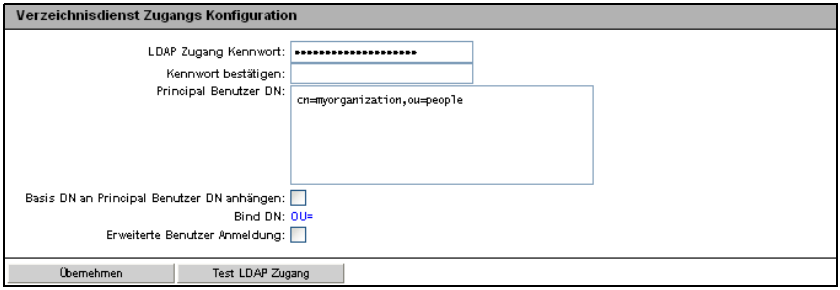


Bild 165: Novell eDirectory / OpenLDAP /OpenDS: Verzeichnisdienst Zugangs Konfiguration

LDAP Zugang Kennwort

Kennwort, mit dem sich der *Principal Benutzer* (Principal User) beim LDAP-Server authentisiert.

Kennwort bestätigen

Wiederholen Sie das unter *LDAP Zugang Kennwort* eingegebene Kennwort.

Principal Benutzer DN

„Fully Distinguished Name“, d.h.vollständige Beschreibung von Objektpfad und der Attributen der generischen iRMC S2/S3-Benutzerkennung (Principal Benutzer), unter der der iRMC S2/S3 vom LDAP-Server die Benutzerberechtigungen der iRMC S2/S3-Benutzer erfragt.

Basis DN an Principal Benutzer DN anhängen

Wenn Sie diese Option aktivieren, brauchen Sie den Basis DN unter *Principal Benutzer DN* nicht anzugeben. Es wird dann der Basis DN verwendet, den Sie in der Gruppe *Globale Verzeichnisdienst Configuration* unter *Basis DN* spezifiziert haben.

Bind DN

Unter *Bind DN* wird der Principal Benutzer DN angezeigt, wie er für die LDAP-Authentifizierung verwendet wird.

Erweiterte Benutzer Anmeldung

Erhöhte Flexibilität bei der Benutzeranmeldung.

Aktivieren Sie diese Option nur, wenn Sie mit der LDAP-Syntax vertraut sind. Wenn Sie versehentlich einen ungültigen Suchfilter spezifizieren und aktivieren, können sich Benutzer erst nach einer Deaktivierung der Option *Erweiterte BenutzerAnmeldung* wieder unter einer globalen Benutzerkennung am iRMC S2/S3 anmelden.

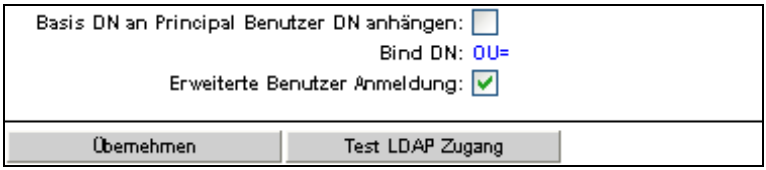


Bild 166: Erweiterte Benutzer Anmeldung“

Wenn Sie *Erweiterte Benutzer Anmeldung* markieren und mit *Übernehmen* aktivieren, wird ein zusätzliches Eingabefeld *Benutzer Such Kriterium* angezeigt, das mit dem Standard-Anmelde-Suchfilter "(&(objectclass=person)(cn=%s))" vorbelegt ist.

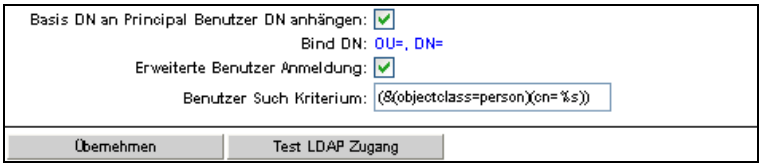


Bild 167: LDAP-Suchfilter für „Erweiterte Benutzer Anmeldung“

Beim Anmelden wird der Platzhalter „%s“ durch die jeweilige globale Benutzerkennung ersetzt. Den Standardfilter können Sie modifizieren, indem Sie z.B. anstatt „cn=“ ein anderes Attribut angeben. Anmeldeberechtigt am iRMC S2/S3 sind dann alle globalen Benutzkennungen, die den Bedingungen dieses Suchfilters genügen.

Test LDAP Zugang

Überprüft die Zugangsdaten zum LDAP-Verzeichnisserver und zeigt als Ergebnis den LDAP-Status an (siehe Bild 168).

Dieser Test prüft lediglich die Basis-Zugangsdaten („LDAP-Server vorhanden?“, „Benutzer konfiguriert?“), führt jedoch keine vollständige Autorisierung des Benutzers durch.

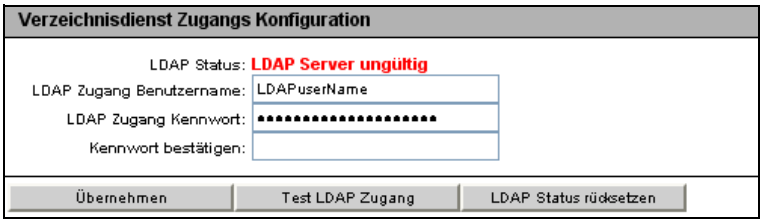


Bild 168: eDirectory/OpenLDAP: Status der Verbindung zum LDAP-Server

- Klicken Sie auf *LDAP Status zurücksetzen*, um die Statusanzeige zurückzusetzen.

- Klicken Sie auf *Übernehmen,* um Ihre Einstellungen zu aktivieren.

- Konfigurieren Sie in der Gruppe *Verzeichnisdienst E-Mail Benachrichtigung Konfiguration* die Einstellungen für globale E-Mail-Benachrichtigung.

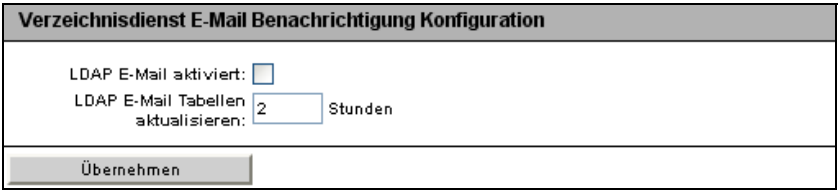


Bild 169: Verzeichnisdienst E-Mail Benachrichtigung Konfiguration

LDAP E-Mail aktiviert

Aktiviert die globale E-Mail-Benachrichtigung.

LDAP E-Mail Tabellen aktualisieren [Stunden]

Definiert das Intervall für die regelmäßige Aktualisierung der E-Mail-Tabelle. Der Wert „0“ bedeutet: keine regelmäßige Aktualisierung.

- Klicken Sie auf *Übernehmen,* um Ihre Einstellungen zu aktivieren.

7.14.3 Centralized Authentication Service (CAS) Konfiguration - CAS Service konfigurieren

Diese Funktion wird nicht für alle PRIMERGY Server mit iRMC S2/S3 unterstützt.

SSO wird nur für den Zugang zum iRMC S2/S3 via Web-Oberfläche unterstützt. SSO wird **nicht** nur für den Zugang zum iRMC S2/S3 via Remote Manager (Telnet/SSH) unterstützt.

Mithilfe der Seite *Centralized Authentication Service (CAS) Konfiguration* können die iRMC S2/S3-Web-Oberfläche für das Single Sign-on (SSO) via CAS Service konfigurieren.

Ruft ein Benutzer zum erstem Mal eine Anwendung der innerhalb der SSO Domäne des CAS Service auf, dann präsentiert ihm der CAS Service das CAS-spezifische Authentisierungsfenster. Nach einmaliger erfolgreicher Authentisierung beim CAS Service hat der Benutzer dann Zugriff auf die iRMC S2/S3-Web-Oberfläche sowie alle anderen Anwendungen der SSO Domäne, ohne sich jedesmal neu einloggen zu müssen.

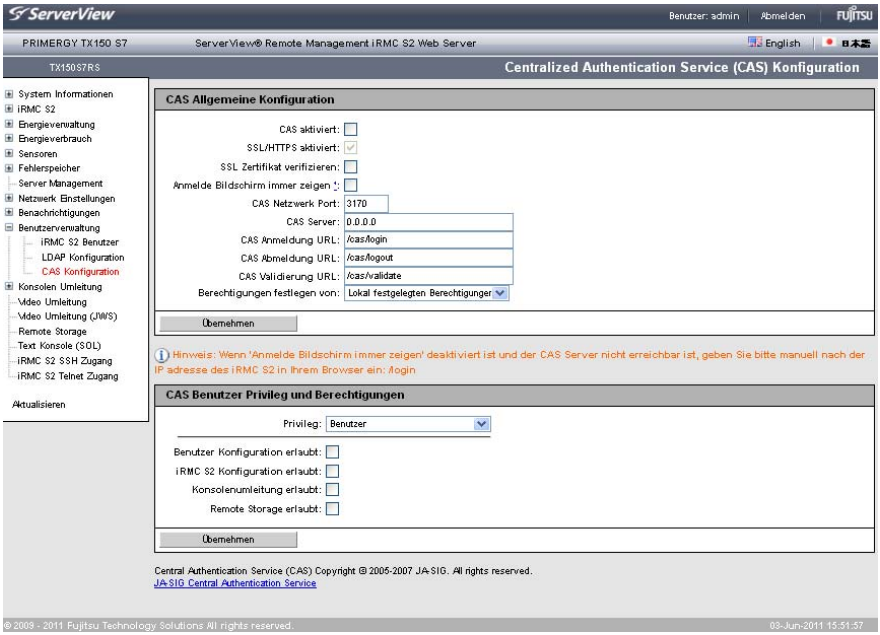


Bild 170: Centralized Authentication Service (CAS) Konfiguration

CAS Allgemeine Konfiguration

In der Gruppe *CAS Allgemeine Konfiguration* konfigurieren Sie den Zugang zu einem CAS service.

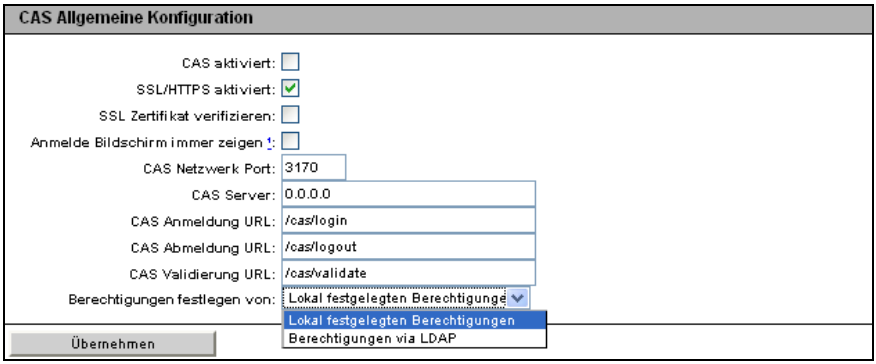


Bild 171: CAS Allgemeine Konfiguration

CAS aktiviert

Aktiviert SSO mithilfe des spezifizierten den CAS Service.

SSL/HTTPS aktiviert

Die Kommunikation zwischen CAS Service und iRMC S2/S3 erfolgt SSL-verschlüsselt.

SSL Zertifikat verifizieren

Das SSL-Zertifikat des CAS Service wird mit Zertifizierungsstellenzertifikat (CA Certificate) abgeglichen.

Anmelde Bildschirm immer zeigen

Wenn *Anmelde Bildschirm immer zeigen* deaktiviert ist und der CAS Server nicht erreichbar ist, geben Sie bitte manuell nach der IP-Adresse des iRMC S2/S3 in Ihrem Browser den String `/login` ein.

Zeigt den Anmelde-Bildschirm des iRMC S2/S3 immer an:

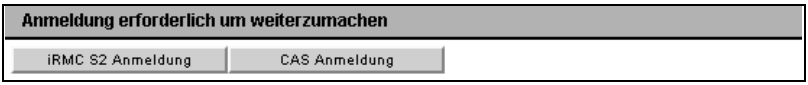


Bild 172: Anmeldebildschirm

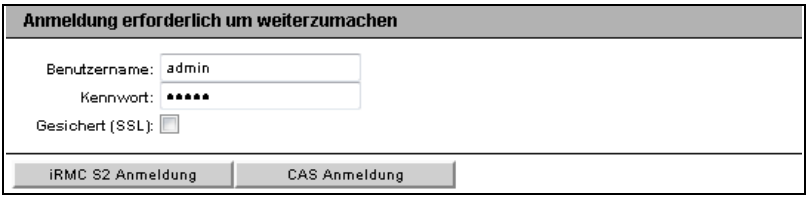


Bild 173: Anmeldebildschirm - explizite Authentisierung erforderlich

Dies ermöglicht es Benutzern, sich temporär am iRMC S2/S3 mit Berechtigungen einzuloggen, die von dem unter *CAS Benutzer Privileg und Berechtigungen* (siehe Seite 301) festgelegten Berechtigungsprofil abweichen.

Wenn z.B. ein Benutzer, der bei CAS unter einer Kennung mit *Benutzer*-Privileg angemeldet ist, eine Aktion ausführen möchte, die das *Administrator*-Privileg erfordert, dann kann er sich am iRMC S2/S3 temporär unter einer entsprechend privilegierten Kennung anmelden. Ein Wechsel zwischen diesen beiden Kennungen ist jedoch nicht möglich.

Die beiden Schaltflächen *iRMC S2/S3 Anmeldung* und *CAS Anmeldung* haben folgende Funktionalität:

iRMC S2/S3 Anmeldung

Meldet den Benutzer - ohne Einschaltung des CAS Service - mit den angegebenen Werten für *Benutzername* und *Passwort* an der iRMC S2/S3-Web-Oberfläche an.

CAS Anmeldung

Meldet den Benutzer via SSO Login an der iRMC S2/S3-Web-Oberfläche an:

- Falls der Benutzer noch nicht vom CAS Service authentifiziert wurde: Der Benutzer wird mit den angegebenen Werten für *Benutzername* und *Passwort* zur Authentifizierung an den CAS Service weitergeleitet.
- Falls der Benutzer bereits vom CAS Service authentifiziert wurde: Der Benutzer wird - ohne Angabe von Benutzername und Passwort - am iRMC S2/S3 eingeloggt.

CAS Netzwerk Port

Port des CAS Service.
Standard-Portnummer: 3170

CAS Server

IP-Adresse des CAS Service.

Es ist zwingend erforderlich, dass alle Systeme, die an der SSO-Domäne teilnehmen, zur Referenzierung der Management-Station eine identische Darstellung der Adressierung verwenden. (Eine SSO-Domäne umfasst alle Systeme bei denen die Authentifizierung über denselben CAS Service abgewickelt wird). Falls Sie z.B. den ServerView Operations Manager unter Verwendung des Namens „my-cms.my-domain“ installiert haben, müssen Sie bei der Konfigurierung des CAS Service für einen iRMC S2/S3 (derselben SSO-Domäne) den identischen Namen verwenden. Würden Sie hingegen lediglich „my-cms" oder die IP-Adresse für my-cms angeben, wäre SSO zwischen dem iRMC S2/S3 und dem Operations Manager nicht möglich.

CAS Anmeldung URL

Anmeldungs-URL des CAS Service.

CAS Abmeldung URL

Logout URL des CAS Service.

CAS Validierung URL

Validierungs-URL des CAS Service.

Berechtigungen festlegen von

Legt die iRMC S2/S3-Berechtigungen für Benutzer fest, die sich via SSO SSO am iRMC S2/S3 einloggen:

Lokal festgelegten Berechtigungen

Für den Benutzer gelten die unter *CAS Benutzer Privileg und Berechtigungen* festgelegten Berechtigungen.

Berechtigungen via LDAP

Für den Benutzer gilt das Berechtigungsprofil, das im LDAP Verzeichnisservice für den Benutzer hinterlegt ist.

Die Option *Berechtigungen via LDAP* steht nur dann zur Verfügung, wenn LDAP aktiviert ist (siehe Option "LDAP aktiviert" auf Seite 283).

CAS Benutzer Privileg und Berechtigungen

In der Gruppe *CAS Benutzer Privileg und Berechtigungen* legen Sie die iRMC S2/S3-Berechtigungen für Benutzer fest, die sich via SSO am iRMC S2/S3 einloggen.

Die Gruppe *CAS Benutzer Privileg und Berechtigungen* wird nicht angezeigt, wenn Sie in der Gruppe *CAS Allgemeine Konfiguration* unter *Berechtigungen festlegen von* die Option *Berechtigungen via LDAP* gewählt haben.

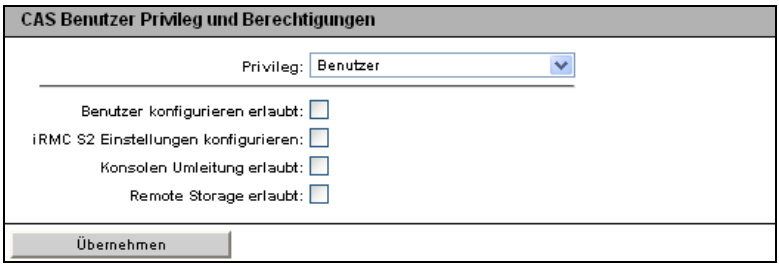


Bild 174: CAS Benutzer Privileg und Berechtigungen

Privileg

Ordnet dem Benutzer eine Berechtigungsgruppe zu:

- *Benutzer*
- *Operator*
- *Administrator*
- *OEM*

Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt "Benutzerberechtigungen" auf Seite 72.

Ergänzend können Sie einem Benutzer individuell folgende Kanal-unabhängigen Berechtigungen erteilen:

Benutzer konfigurieren erlaubt

Berechtigt zum Konfigurieren von lokalen Benutzerzugangsdaten.

iRMC S2/S3 Einstellungen konfigurieren

Berechtigt zum Konfigurieren der iRMC S2/S3-Einstellungen.

Konsolen Umleitung erlaubt

Berechtigt zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection, AVR) im „Nur Lesen“- und „Volle Kontrolle“-Modus.

Remote Storage erlaubt

Berechtigt zur Nutzung der Remote Storage-Funktionalität.

7.15 Konsolen-Umleitung

Bei der Konsolen-Umleitung können Sie zwischen folgenden Seiten wählen:

- "BIOS Text Konsole - Text-Konsolen-Umleitung konfigurieren und starten" auf Seite 302.
- "Grafische Konsolen Umleitung (AVR) - Grafische Konsolen-Umleitung (AVR) starten" auf Seite 312.

7.15.1 BIOS Text Konsole - Text-Konsolen-Umleitung konfigurieren und starten

Mithilfe der Seite *BIOS Text Konsole* können Sie die Text-Konsolen-Umleitung konfigurieren und starten.

Die Text-Konsolen-Umleitung können Sie auch im BIOS konfigurieren (siehe Abschnitt "Text-Konsolen-Umleitung via LAN über das BIOS / TrustedCore / UEFI Setup Utility konfigurieren" auf Seite 50).

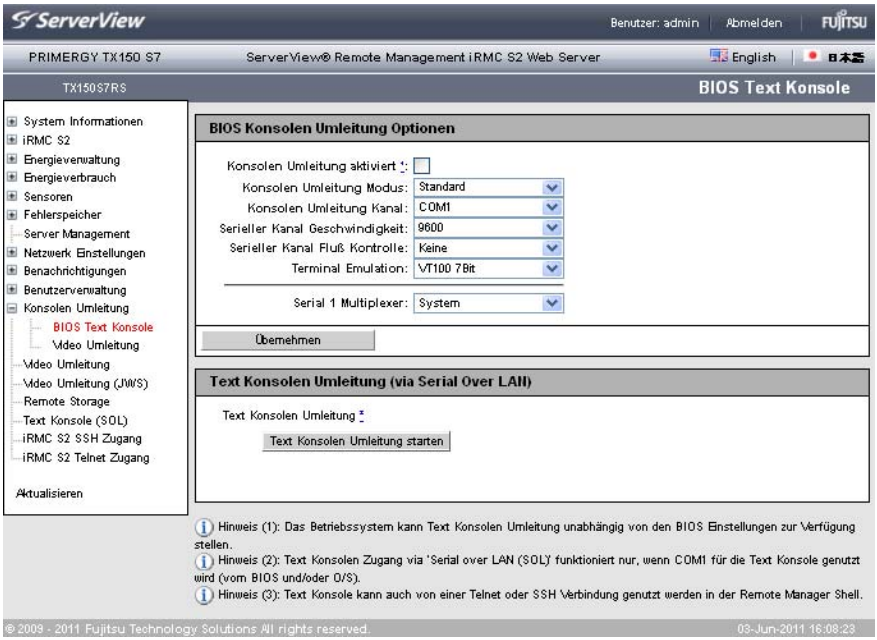


Bild 175: Seite BIOS Text Konsole

7.15.1.1 BIOS Konsolen Umleitung Optionen - Text-Konsolen-Umleitung konfigurieren

Unter *BIOS Konsolen Umleitung Optionen* können Sie die Text-Konsolen-Umleitung konfigurieren.

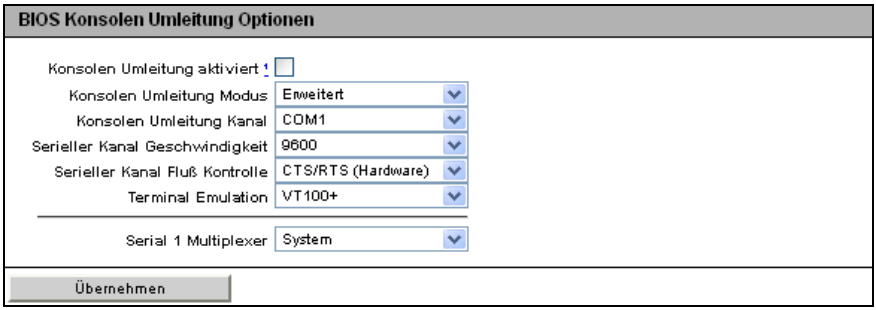


Bild 176: Seite BIOS Text Konsole - BIOS Konsolen Umleitung Optionen

Konsolen Umleitung aktiviert

Mit dieser Option aktivieren/deaktivieren Sie die Konsolen-Umleitung.

Das Betriebssystem kann die Text-Konsolen-Umleitung auch unabhängig von den Einstellungen im BIOS ermöglichen.

Konsolen Umleitung Modus

Diese Einstellung wirkt sich auf das Verhalten der Konsolen-Umleitung bei laufendem Betriebssystem (nach der BIOS POST-Phase) aus (siehe Abschnitt "Text-Konsolen-Umleitung bei laufendem Betriebssystem" auf Seite 310):

Standard

Die Konsolen-Umleitung wird nach der POST-Phase des BIOS beendet.

Erweitert

Die Konsolen-Umleitung steht über die POST-Phase des BIOS hinaus zur Verfügung.

Konsolen Umleitung Kanal

Es stehen zwei serielle Kanäle (Ports) zur Verfügung: *Serial 1*, *Serial 2*.

Wenn die Konsolen-Umleitung über LAN funktionieren soll, muss *Serial 1* eingestellt sein.

Wenn *Serial 2* ausgewählt ist, funktioniert nur der Anschluss über Nullmodem-Kabel.

Serieller Kanal Geschwindigkeit

Folgende Geschwindigkeiten (Baud Rates) können eingestellt werden: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Serieller Kanal Flusskontrolle

Folgende Einstellungen sind möglich:

Keine

Die Flusskontrolle ist ausgeschaltet.

XON/XOFF (Software)

Die Flusskontrolle wird via Software durchgeführt.

CTS/RTS (Hardware)

Die Flusskontrolle wird via Hardware durchgeführt.

Terminal Emulation

Es werden folgende Terminal Emulationen angeboten:

VT100 7Bit, VT100 8Bit, PC-ANSI 7Bit, PC-ANSI 8 Bit, VT100+, VT-UTF8

Serial 1 Multiplexer

Prüfen Sie die Multiplexer-Einstellungen auf Konsistenz:

- Serial: System
- LAN: iRMC S2/S3

► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

7.15.1.2 Text Konsolen Umleitung (via Serial Over LAN) - Text-Konsolen-Umleitung starten

Unter *Text Konsolen Umleitung (via Serial Over LAN)* können Sie die Text-Konsolen-Umleitung starten.

Die Text-Konsolen-Umleitung via Serial Over LAN (SOL) setzt voraus, dass Betriebssystem und/oder BIOS den seriellen Kanal (Port) 1 (COM1) für die Umleitung der Text-Konsole verwenden.

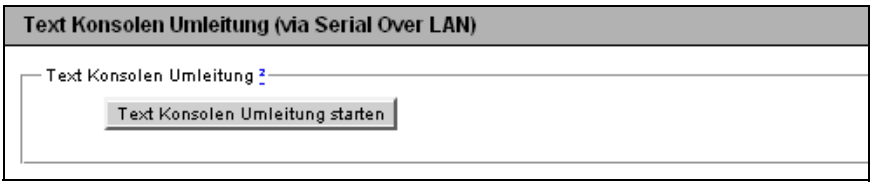


Bild 177: Text-Konsolen-Umleitung via Serial Over LAN (SOL) starten

- Klicken Sie auf die Schaltfläche *Text Konsolen Umleitung Starten*, um die Text-Konsolen-Umleitung zu starten.

  Das JAVA-Applet für die Text-Konsolen-Umleitung wird gestartet (siehe Bild 178 auf Seite 306):

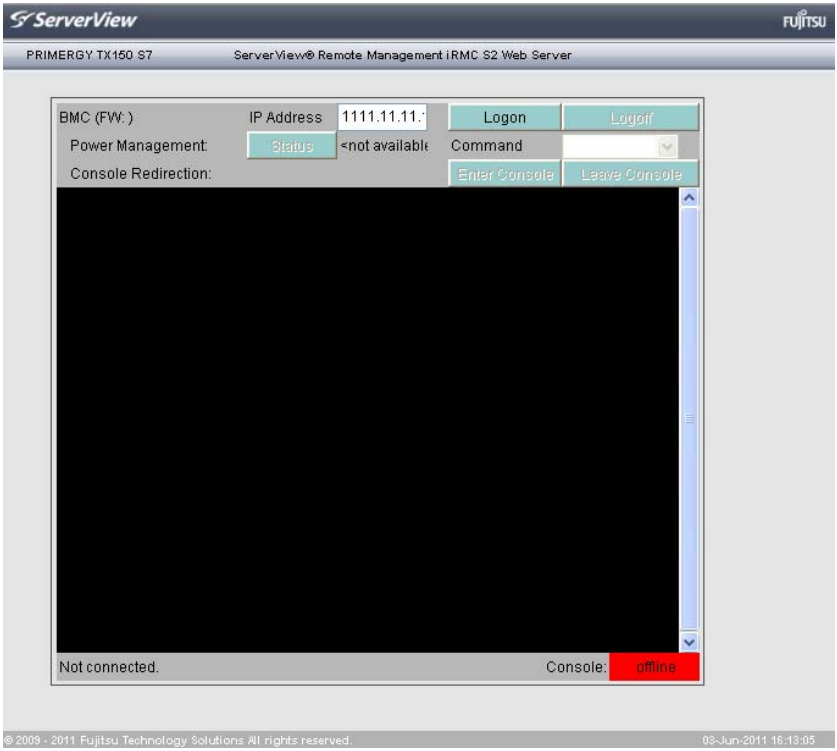


Bild 178: Fenster für Energieverwaltung und Text-Konsolen-Umleitung (vor Logon)

► Klicken Sie auf die Schaltfläche *Logon*, um sich am iRMC S2/S3 anzumelden.

Anschließend werden Sie zur Eingabe von iRMC S2/S3-Benutzerkennung und -Kennwort aufgefordert:

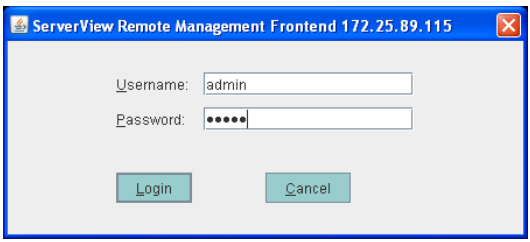


Bild 179: Energieverwaltung und Text-Konsolen-Umleitung - Anmelde-Fenster

► Geben Sie Benutzerkennung und Kennwort ein und bestätigen Sie durch Klicken auf *Login*.

Anschließend wird das Fenster für Energieverwaltung und Text-Konsolen-Umleitung angezeigt:

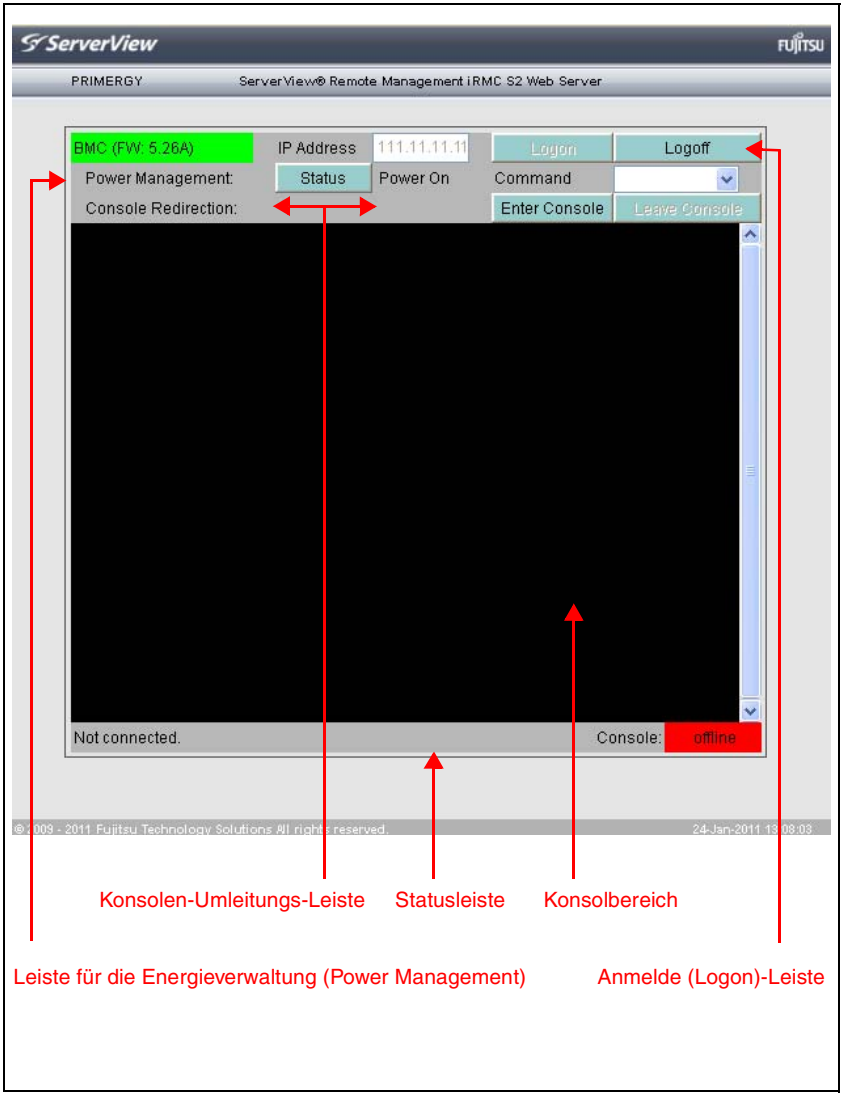


Bild 180: Fenster für Energieverwaltung und Text-Konsolen-Umleitung

Nachfolgend sind die Elemente des Konsolen-Umleitungs-Fensters erläutert:

Anmelde (Logon)-Leiste
: In der Anmelde-Leiste werden IP-Adresse und aktuelle Firmware-Version des iRMC S2/S3 angezeigt. Über die Schaltflächen *Logon* und *Logout* können Sie sich am iRMC S2/S3 anmelden bzw. abmelden.

Leiste für die Energieverwaltung (Power Management)
: Die Leiste für die Energieverwaltung informiert über den Energie-Status (Power Status) des verwalteten Servers. Mithilfe der Schaltfläche *Status* können Sie die Anzeige aktualisieren.

  In der Dropdown-Liste *Command* können Sie ein IPMI-Kommando für das Power Management des verwalteten Servers auswählen und starten (siehe Seite Seite 309). Hierfür müssen Sie nicht mit der Konsole verbunden sein.

Konsolen-Umleitungs-Leiste
: In der Konsolen-Umleitungs-Leiste können Sie mithilfe der Schaltflächen *Enter Console* und *Leave Console* die Anzeige im Konsolbereich ein- bzw. ausschalten.

Konsolen-Bereich
: Der Konsolen-Bereich enthält die Anzeigen der umgeleiteten Text-Konsole.

Statusleiste
: Die Statusleiste zeigt die IP-Adresse des iRMC S2/S3 sowie die Portnummer für die Konsolen-Umleitung an. Außerdem informiert die Statusleiste über den Status der Konsolen-Umleitung (online/offline).

► Klicken Sie auf *Enter Console*.

Danach sind Sie mit der Konsole verbunden und können das gewünschte Kommando ausführen, indem Sie es entweder direkt im Konsolbereich eingeben oder in der Dropdown-Liste *Command* (nur IPMI-Kommandos) anklicken:

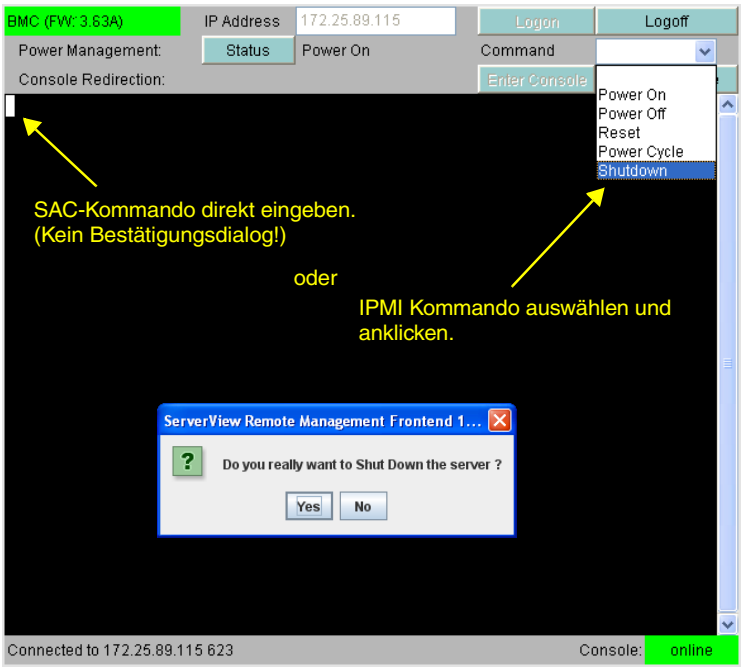


Bild 181: SAC- oder IPMI-Kommandos an der Text-Konsole eingeben.

IPMI-Kommando	Erläuterung
Power On	Schaltet den Server ein.
Power Off	Schaltet. den Server aus.
Reset	Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).
Power Cycle	Schaltet den Server vollständig aus und nach ca. 5 Sekunden wieder ein.
Shutdown	Fährt den Server „sanft“ herunter und schaltet ihn aus.

► Um die Verbindung zur Konsole zu beenden, klicken Sie auf die Schaltfläche *Leave Console*.

7.15.1.3 Text-Konsolen-Umleitung bei laufendem Betriebssystem

Sie können - je nach Betriebssystem des verwalteten Servers - auch nach der BIOS POST-Phase noch die Konsolen-Umleitung nutzen.

DOS

Bedingung:

Die BIOS-Einstellung für den Modus der Konsolen-Umleitung muss auf *Enhanced* konfiguriert sein (siehe Abschnitt "BIOS Text Konsole - Text-Konsolen-Umleitung konfigurieren und starten" auf Seite 302).

Wenn der verwaltete Server in Folge eines Problems die ServerView Suite/ Diagnose-Software startet, können Sie ServerView Suite/Diagnose remote über eine Konsolen-Umleitung bedienen.

Windows Server 2003

Windows Server 2003 übernimmt nach der POST-Phase automatisch die Konsolen-Umleitung, ohne dass weitere Einstellungen notwendig sind. Während der Start-Phase des Betriebssystems wird die SAC-Konsole von Windows Server 2003 übertragen:

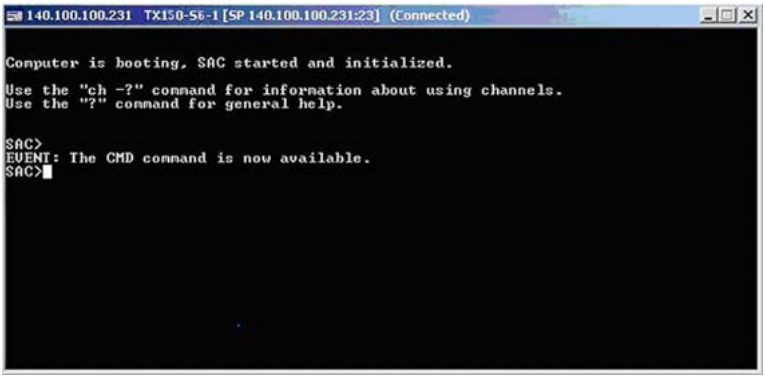

140.100.100.231 TX150-S6-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: The CMD command is now available.
SAC>

Bild 182: SAC-Konsole von Windows Server 2003

Linux

Ein Linux-Betriebssystem müssen Sie konfigurieren, damit es die Konsolen-Umleitung nach der POST-Phase übernimmt. Wenn es konfiguriert ist, haben Sie remote vollen Zugriff.

Notwendige Einstellungen

Die Einstellungen können sich je nach Programmversion etwas ändern.

SuSe und RedHat

Fügen Sie am Ende der Datei */etc/inittab* folgende Zeile an:

```
xx:12345:respawn:/sbin/agetty <baudrate> ttyS0
```

RedHat

Fügen Sie in die Datei */etc/grub.conf* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

SuSE

Fügen Sie in die Datei */boot/grub/menu.lst* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baudrate> console=tty0
```

7.15.2 Grafische Konsolen Umleitung (AVR) - Grafische Konsolen-Umleitung (AVR) starten

Mithilfe der Seite *Grafische Konsolen Umleitung (Advanced Video Redirection)* können Sie die grafische Konsolen-Umleitung starten. Die Funktion „Grafische Konsolen-Umleitung (Advanced Video Redirection, AVR)“ leitet die grafische Ausgabe des verwalteten Servers zum Remote-Arbeitsplatz um und ordnet die Tastatur- und Mauseingaben des Remote-Arbeitsplatzes dem verwalteten Server zu, sodass Sie am Remote-Arbeitsplatz so auf den verwalteten Server zugreifen können, als bedienten Sie ihn vor Ort.

Die grafische Konsolen-Umleitung kann von zwei Benutzern gleichzeitig verwendet werden. Dabei hat ein Benutzer die volle Kontrolle über den Server („Volle Kontrolle“-Modus), während der andere Benutzer die Bedienung des Servers via die Tastatur- und Mauseingaben nur passiv verfolgen kann („Nur Lesen“-Modus).

Um die iRMC S2/S3-Funktion *Grafische Konsolen Umleitung (AVR)* nutzen zu können, benötigen Sie einen Lizenzschlüssel (siehe "Lizenzschlüssel (License Key) auf den iRMC S2/S3 laden." auf Seite 172).

Die Funktionalität der Grafischen Konsolen-Umleitung wird über ein Java Applet zur Verfügung gestellt.

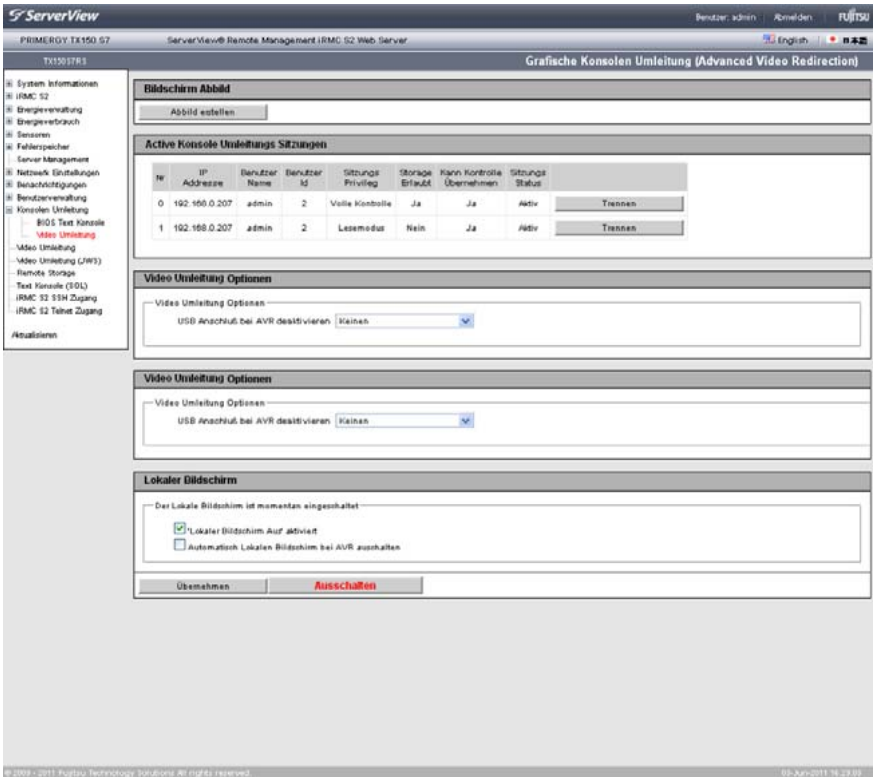


Bild 183: Seite Grafische Konsolen Umleitung (Advanced Video Redirection)

Bildschirm- Abbild erstellen

Unter *Bildschirm Abbild* können Sie

– ein Bildschirm-Abbild (Screenshot) des aktuellen VGA-Bildschirms am verwalteten Server erstellen und in der Firmware des iRMC S2/S3 abspeichern,

– das in der iRMC S2/S3-Firmware gespeicherte Bildschirm-Abbild ansehen,

– das in der iRMC S2/S3-Firmware gespeicherte Bildschirm-Abbild löschen.

Bild 184: Bildschirm-Abbild ansehen / erstellen / löschen

Bei ASR&R-Ereignissen - dies sind typischerweise Watchdog-Ereignisse oder „Blue Screen“ am verwalteten Server - wird automatisch ein Bildschirm-Abbild erstellt.

In der Firmware der iRMC S2/S3 ist maximal **ein** Bildschirm-Abbild gespeichert, und zwar das zuletzt erstellte Bildschirm-Abbild.

Durch Klicken auf eine der angezeigten Schaltflächen, können Sie folgende Aktionen durchführen:

Abbild anschauen
(Wird nur angezeigt, wenn ein Bildschirm-Abbild gespeichert ist.)
Das Bildschirm-Abbild wird in einem separaten Browser-Fenster angezeigt.

Abbild Vorschau
(Wird nur angezeigt, wenn ein Bildschirm-Abbild gespeichert ist.)
Eine verkleinerte Vorschau des Bildschirm-Abbilds wird in der Gruppe *Bildschirm Abbild* angezeigt.

Abbild erstellen
Es wird ein neues Bildschirm-Abbild erstellt.

Abbild löschen
(Wird nur angezeigt, wenn ein Bildschirm-Abbild gespeichert ist.)
Nach einem Bestätigungsdialog wird das Bildschirm-Abbild gelöscht, das in der iRMC S2/S3-Firmware gespeichert ist.

Aktive Konsolen Umleitungs Sitzungen

Unter *Aktive Konsolen Umleitungs Sitzungen* werden die zurzeit aktiven AVR-Sitzungen aufgelistet. Falls aktuell keine AVR-Sitzung aktiv ist, wird die Gruppe *Aktive Konsolen Umleitungs Sitzungen* nicht angezeigt.

Wenn aktuell zwei AVR-Sitzungen aktiv sind, wird zu jeder Sitzung eine Schaltfläche *Trennen* angezeigt.

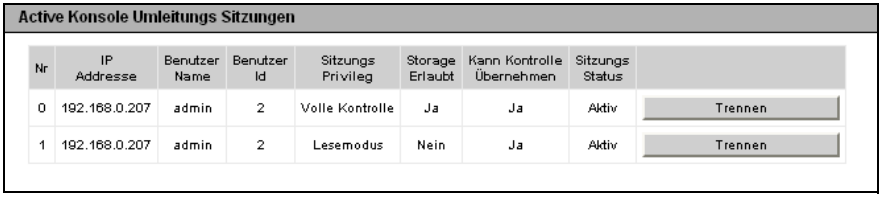


Bild 185: Aktive Konsolumleitungen Sitzungen (zwei aktive Sitzungen)

Trennen

Durch Klicken auf eine Schaltfläche *Trennen* können Sie in einem Bestätigungsdialog die links neben dieser Schaltfläche angezeigte AVR-Sitzung beenden.

Mit *Trennen* können Sie nur AVR-Sitzungen anderer Benutzer beenden. Um Ihre eigene Sitzung zu beenden, wählen Sie im AVR-Fenster: Menü *Extras* - *Beenden* (siehe Seite 109).

Video Umleitung Optionen - USB-Anschlüsse am verwalteten Server für die Dauer der AVR-Sitzung deaktivieren

Diese Funktion wird nicht für alle PRIMERGY Server unterstützt.

Unter *Video Umleitung Optionen - USB Anschluss bei AVR deaktivieren* legen Sie fest, welche USB-Anschlüsse am verwalteten Server für die Dauer der AVR-Sitzung deaktiviert werden sollen.

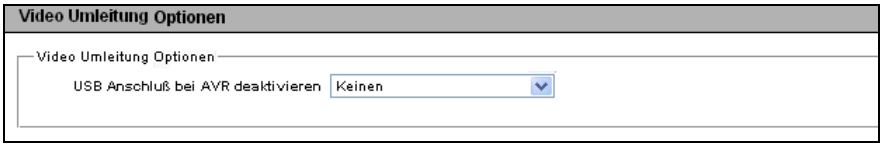


Bild 186: Video Umleitung Optionen

Keinen
Kein USB-Anschluss wird deaktiviert.

Vorderen USB
Nur der USB-Anschluss auf der Frontseite des Servers wird deaktiviert.

Hinteren USB
Nur der USB-Anschluss auf der Rückseite des Servers wird deaktiviert.

Alle Deaktivieren
Alle USB-Anschlüsse des verwalteten Servers werden deaktiviert.

► Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

Lokaler Bildschirm - Ein-/Ausschalt-Optionen für den Server-lokalen Bildschirm festlegen

Unter *Lokaler Bildschirm* wird der Status des lokalen Bildschirms am verwalteten Server angezeigt (siehe Abschnitt "„Lokaler Bildschirm Aus“-Funktionalität" auf Seite 97).

Darüber hinaus können Sie konfigurieren,

– dass sich der lokale Bildschirm vom Remote-Arbeitsplatz aus ein- und ausschalten lässt,

– dass sich der lokale Bildschirm beim Start einer AVR-Sitzung automatisch für die Dauer der AVR-Sitzung ausschaltet.

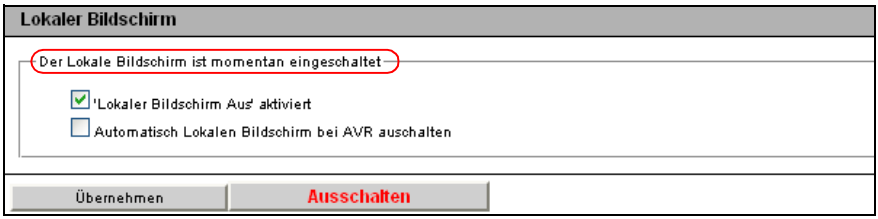


Bild 187: Seite Grafische Konsolen Umleitung- Lokaler Bildschirm

Wenn am verwalteten Server ein Grafikmodus mit hohe Auflösung (High Resolution Mode) eingestellt ist (siehe Tabelle 3 auf Seite 92), ist der lokale Bildschirm aus Performance-Gründen für die Dauer einer AVR-Sitzung immer ausgeschaltet und kann nicht eingeschaltet werden. Außerdem lassen sich keine Einstellungen konfigurieren. Dies wird durch eine entsprechende Meldung angezeigt.

'Lokaler Bisdschirm Aus' aktiviert

Mit dieser Option aktivieren Sie die folgenden Möglichkeiten:

– Im „Volle Kontrolle“-Modus einer AVR-Sitzung können Sie den lokalen Bildschirm aus- und einschalten (AVR-Menü *Extras*, siehe Seite 109).

– Für **Benutzer mit Administrator- oder OEM-Berechtigung** ist außerdem die alternierende Schaltfläche *Ausschalten* / *Einschalten* aktiviert, über die sich der lokale Bildschirm ebenfalls aus- und einschalten lässt (siehe Bild 188).

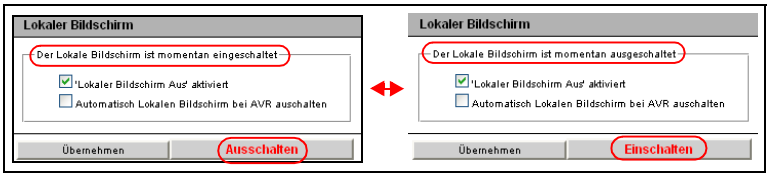


Bild 188: Seite Grafische Konsolen Umleitung - Lokaler Bildschirm Ein/Aus

– Zusätzlich können Sie konfigurieren, dass sich der lokale Bildschirm automatisch beim Start einer AVR-Sitzung für die Dauer dieser AVR-Sitzung ausschaltet (siehe Option *Automatisch Lokalen Bildschirm bei AVR ausschalten* auf Seite 318).

Sofern nicht eine parallele AVR-Sitzung mit *'Lokaler Bildschirm aus' aktiviert* aktiv ist, schaltet sich der lokale Bildschirm beim Beenden der AVR-Sitzung automatisch wieder ein.

Automatisch Lokalen Bildschirm bei AVR ausschalten

Diese Option ist nur wirksam, wenn die Option *'Lokaler Bildschirm aus' aktiviert* aktiviert ist.

Wenn Sie diese Option aktivieren, schaltet sich der lokale Bildschirm jeweils beim Start einer AVR-Sitzung automatisch für die Dauer dieser AVR-Sitzung aus. Nach Beenden der AVR-Sitzung schaltet sich der lokale Bildschirm automatisch wieder ein, sofern keine weitere AVR-Sitzung mit *'Lokaler Bildschirm aus' aktiviert* aktiv ist.

Parallele AVR-Sitzungen:

Auch wenn Sie während Ihrer AVR-Sitzung den lokalen Bildschirm einschalten (im AVR-Menü *Extras* oder über *Einschalten*), schaltet sich der lokale Bildschirm beim Start einer neuen, parallelen AVR-Sitzung automatisch wieder aus.

Wenn alle AVR-Sitzungen beendet sind, schaltet sich der lokale Bildschirm automatisch wieder ein.

- Klicken Sie auf die Schaltfläche *Übernehmen,* um Ihre Einstellungen zu aktivieren.

Video Umleitung- AVR starten

Unter *Video Umleitung* starten Sie die grafische Konsolen-Umleitung (AVR).

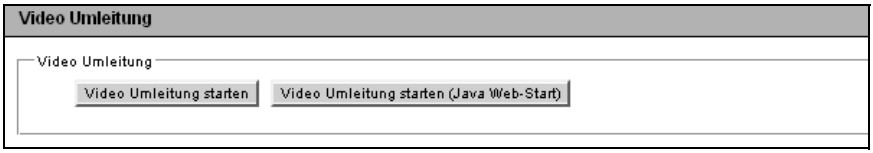


Bild 189: Seite Grafische Konsolen Umleitung - Video Umleitung starten

► Klicken Sie auf die Schaltfläche *Video Umleitung Starten* oder *Video Umleitung Starten (Java Web Start),* um eine (zweite) AVR-Sitzung zu starten.

Das Java-Applet für die grafische Konsolen-Umleitung wird gestartet.

Wenn ein anderer Benutzer die AVR bereits im „Volle Kontrolle“-Modus nutzt, zeigt das Java-Applet das AVR-Fenster im „Nur Lesen“-Modus an. Andernfalls zeigt das Java-Applet das AVR-Fenster im „Volle Kontrolle“-Modus an.

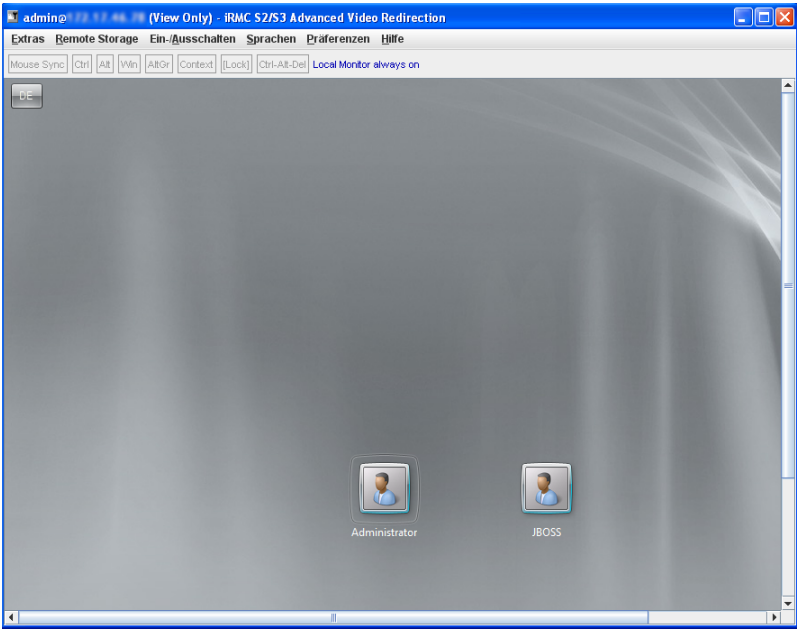

admin@ (View Only) - iRMC S2/S3 Advanced Video Redirection
Extras Remote Storage Ein-/Ausschalten Sprachen Präferenzen Hilfe
Mouse Sync Ctrl Alt Win AltGr Context Lock Ctrl-Alt-Del Local Monitor always on
DE
Administrator
JBOSS

Bild 190: AVR-Fenster („Nur Lesen“-Modus)

► Wählen Sie im AVR-Menü *Extras* - *Kontrolle übernehmen* (Einzelheiten siehe Seite 109), um die volle Kontrolle über den verwalteten Server zu erlangen.

Eine bereits existierenden Sitzung im „Voller Kontrolle“-Modus wird ü über ihren Versuch informiert, die volle Kontrolle über den verwalteten Server zu erlangen.

Falls die „Volle Kontrolle“-Sitzung Ihren Versuch ablehnt, verbleiben Sie im „Nur Lesen“-Modus. Die Benutzer sollten sich über den Modus Ihrer Sitzungen absprechen.

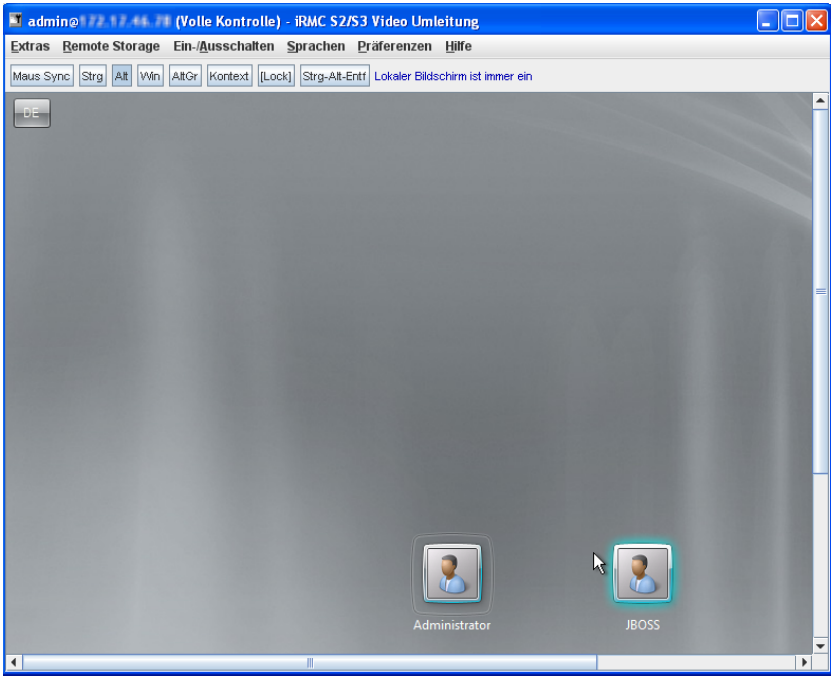

admin@ (Volle Kontrolle) - iRMC S2/S3 Video Umleitung
Extras Remote Storage Ein-/Ausschalten Sprachen Präferenzen Hilfe
Maus Sync Strg Alt Win AltGr Kontext [Lock] Strg-Alt-Entf Lokaler Bildschirm ist immer ein
DE
Administrator
JBOSS

Bild 191: AVR-Fenster („Volle Kontrolle“-Modus)

Die Menüs des AVR-Fensters sowie die integrierten Sondertasten sind im Kapitel "Grafische Konsolen-Umleitung (AVR)" auf Seite 91 beschrieben.

Auf der Seite *Grafische Konsolen Umleitung (AVR)* werden die zurzeit aktiven AVR-Sitzungen wie folgt angezeigt:

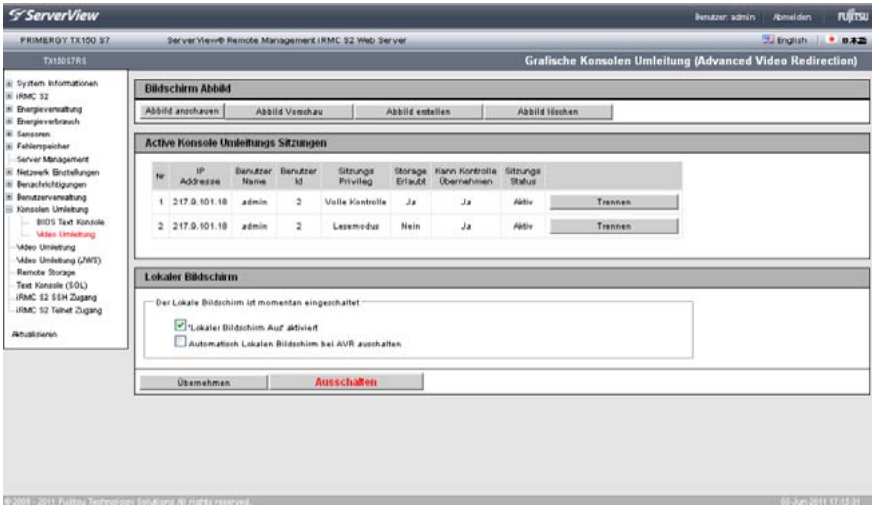


Bild 192: Seite Grafische Konsolen Umleitung bei zwei aktiven AVR-Sitzungen

Trennen

Durch Klicken auf eine Schaltfläche *Trennen* können Sie in einem Bestätigungsdialog die links neben dieser Schaltfläche angezeigte AVR-Sitzung beenden.

Mit *Trennen* können Sie nur AVR-Sitzungen anderer Benutzer beenden. Um Ihre eigene Sitzung zu beenden, wählen Sie im AVR-Fenster: Menü *Extras* - *Beenden* (siehe Seite 109).

Falls der verwaltete Server ausgeschaltet ist, wird das folgende Fenster angezeigt:

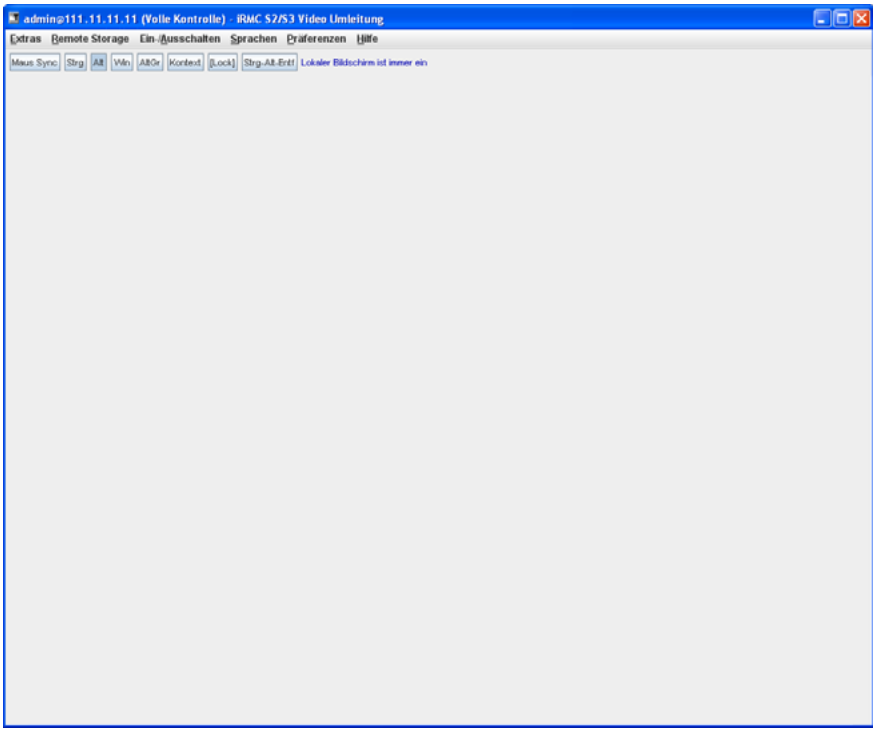


Bild 193: AVR-Fenster bei ausgeschaltetem Server

7.16 Remote Storage

Die Funktion „Remote Storage“ stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich physisch an anderer Stelle im Netz befindet. Die Quelle für das virtuelle Laufwerk kann ein physisches Laufwerk (Disketten-Laufwerk, CD-ROM/DVD-ROM) oder ein ISO-Abbild (Image-Datei) sein.

Um die iRMC S2/S3-Funktion *Remote Storage* nutzen zu können, benötigen Sie einen gültigen Lizenzschlüssel (siehe Seite 174).

Die Remote Storage-Speichermedien stellen Sie wahlweise wie folgt zur Verfügung:

– Am Remote Arbeitsplatz als physisches Laufwerk oder Image-Datei (siehe Seite 119). Die Image-Datei kann außerdem ein Netzlaufwerk sein (mit Laufwerksbuchstaben, z.B. „D:“ für Laufwerk D).

– Über einen Remote Storage Server zentral im Netz als Image-Datei (siehe Seite 133).

Parallele Remote Storage-Verbindungen:

Zur selben Zeit möglich sind entweder

– **maximal zwei** Remote Storage-Verbindungen zu virtuellen Laufwerken am Remote-Arbeitsplatz (bei Verbindungsaufbau via AVR Java-Applet)

oder

– **eine** Remote Storage-Verbindung zu einem Remote Storage Server.

Remote Storage-Verbindungen via Applet und Remote Storage Server sind nicht gleichzeitig möglich.

Mithilfe der Seite *Remote Storage* können Sie sich den Status der aktuellen Remote Storage-Verbindungen anzeigen lassen und außerdem die Verbindung zu einem Remote Storage Server herstellen.

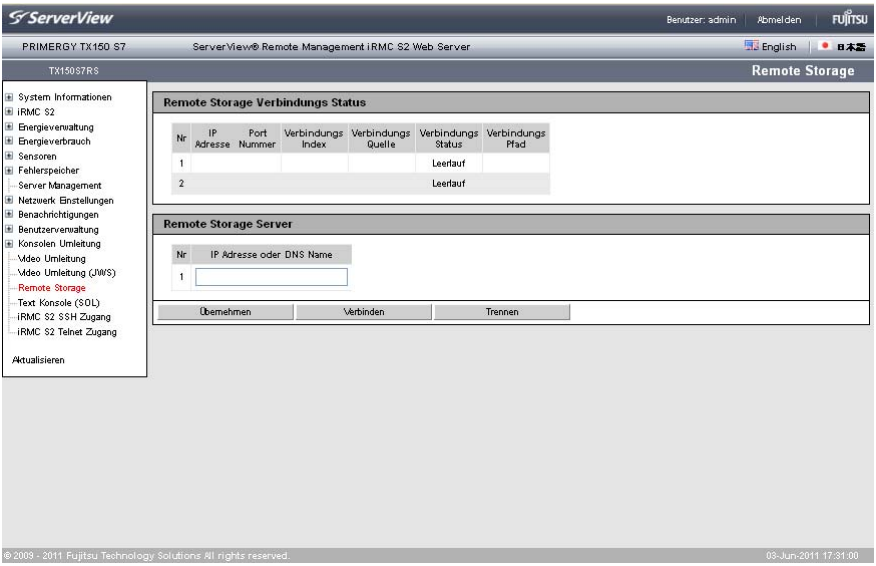


Bild 194: Seite Remote Storage

Remote Storage Verbindungs Status

Zeigt den Status der Remote Storage-Verbindung an.

Nr

Fortlaufende Nummer des Remote Storage-Gerätes.

IP Address

IP-Adresse des Servers / des Arbeitsplatzes, auf dem das Remote Storage-Gerät installiert ist.

Verbindungs-Index

Fortlaufende Nummer, die der Remote Storage-Verbindung zugewiesen ist.

Verbindungs-Quelle

Status des Remote Storage-Gerätes, das sich auf einem Server oder Remote-Arbeitsplatz befindet:

- *Applet*: Verbindung möglich
- *None*: Verbindung nicht möglich (nicht gefunden)

Verbindungs-Status

Status der Verbindung:

- *Verbunden*: Verbindung hergestellt
- *Leerlauf*: Nicht verbunden

Remote Storage Server

Hier geben Sie den Computer an, auf dem der Remote Storage Server läuft.

Nr

Zeigt die fortlaufende Nummer des Remote Storage Servers an

IP Addresse oder DNS Name

IP-Adresse oder den DNS-Namen des Computers ein, auf dem ein Remote Storage Server installiert ist.

Übernehmen

Wenn Sie auf die Schaltfläche *Übernehmen* klicken, wird die IP-Adresse bzw. der DNS-Name des Remote Storage Servers gespeichert.

Verbinden

Wenn Sie auf die Schaltfläche *Verbinden* klicken, wird die IP-Adresse bzw. der DNS-Name des Remote Storage Servers gespeichert und die Verbindung zum Remote Storage Server hergestellt.

Der Verbindungsaufbau zum Remote Storage Server setzt voraus, dass der Remote Storage Server installiert ist und zurzeit ausgeführt wird.

Trennen

Durch Klicken auf die Schaltfläche *Trennen* beenden Sie die Verbindung zum Remote Storage Server.

7.17 iRMC S2/S3 über Telnet / SSH (Remote Manager) bedienen

Für den iRMC S2/S3 gibt es eine Telnet/SSH-basierte Oberfläche - den so genannten Remote Manager. Die alphanumerische Bedienoberfläche des Remote Manager bietet Ihnen u.a. Zugriff auf System-und Sensorinformationen, die Energieverwaltung (Power Management) und den Fehlerspeicher (System Eventlog, SEL). Außerdem können Sie die Text-Konsolen-Umleitung sowie eine SMASH CLP Shell starten.

Von der iRMC S2/S3-Web-Oberfläche aus rufen Sie den Remote Manager wie folgt auf:

– Über den Verweis *iRMC S2/S3 SSH Zugang* im Navigationsbereich initiieren Sie eine durch SSH (**S**ecure **Sh**ell) kryptografisch abgesicherte Telnet-Verbindung zum iRMC S2/S3.

– Über den Verweis *iRMC S2/S3 Telnet Zugang* im Navigationsbereich initiieren Sie eine nicht-gesicherte Telnet-Verbindung zum iRMC S2/S3.

Beim Aufruf des Remote Manager via iRMC S2/S3-Web-Oberfläche wird automatisch ein Java-Applet gestartet, das einen Telnet/SSH-Client implementiert. Dies ermöglicht einen komfortablen Zugang zum Remote Manager, da z.B. mit Windows Betriebssystemen kein SSH-Client ausgeliefert wird. Sie können jedoch auch über jeden beliebigen anderen Telnet- oder SSH-Client auf den Remote Manager zugreifen.

Wenn Sie eine Sie eine SSH-Verbindung über das Java-Applet aufbauen, wird Public Key-Authentifizierung nicht unterstützt.

Maximale Anzahl paralleler Sitzungen:

– Telnet: maximal 4
– SSH: maximal 4
– Telnet und SSH insgesamt: maximal 4

Die Bedienung des iRMC S2/S3 über den Remote Manager ist beschrieben im Kapitel "iRMC S2/S3 über Telnet/SSH (Remote Manager)" auf Seite 333.

Voraussetzung am verwalteten Server

Für den iRMC S2/S3 muss der Zugriff über Telnet aktiviert sein (siehe Abschnitt "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 252).

Der Zugang über das Telnet-Protokoll ist aus Sicherheitsgründen standardmäßig deaktiviert, da Kennwörter im Klartext übertragen werden.

SSH/Telnet-Verbindung aufbauen und beim Remote Manager einloggen

Wenn sich Bildschirm-Anzeigen für SSH- und Telnet-Verbindungen nur in den verbindungsspezifischen Anzeigen (Telnet oder SSH) unterscheiden, ist im Folgenden die Anzeige für eine SSH-Verbindung dargestellt.

► Klicken Sie im der Navigationsbereich auf den Verweis *iRMC S2S2/S3 /S3 SSH Zugang* (SSH) bzw. *iRMC S2/S3 Telnet Zugang* (Telnet).

Das Java-Applet für die SSH- bzw. Telnet-Verbindung wird gestartet und das folgende Fenster angezeigt (hier am Beispiel einer SSH-Verbindung):

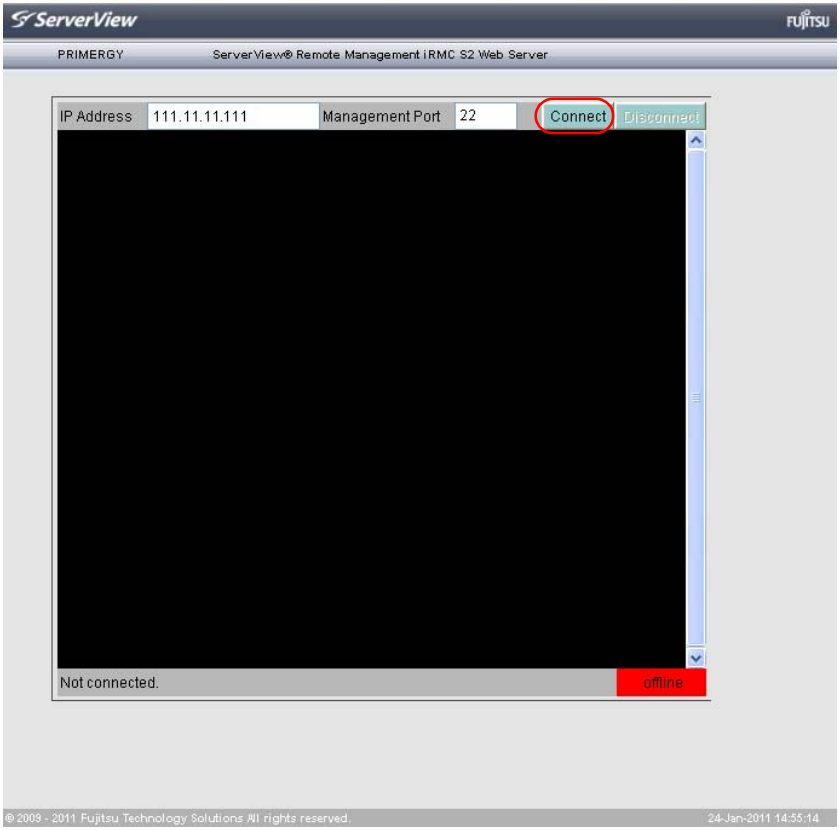


Bild 195: SSH-Verbindung zum iRMC S2/S3 aufbauen

► Klicken Sie in der Verbindungsleiste auf die Schaltfläche *Connect*.

Sobald die Verbindung zum iRMC S2/S3 aufgebaut ist, werden Sie zur Eingabe von Benutzerkennung und Kennwort aufgefordert:

– *Einloggen beim Remote Manager über eine SSH-Verbindung*

Falls der Host-Key des verwalteten Servers noch nicht am Remote-Arbeitsplatz registriert ist, meldet der SSH-Client einen Security-Alert mit Vorschlägen für das weitere Vorgehen.

Es wird das folgende Anmeldefenster angezeigt:

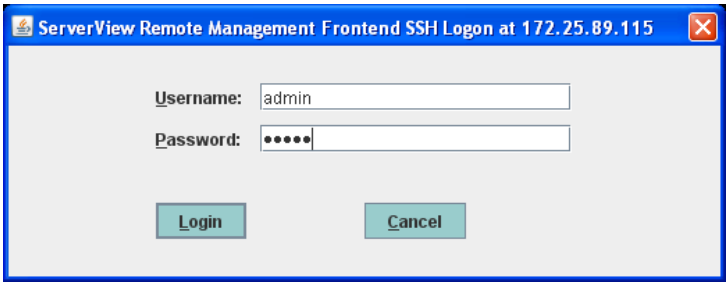


Bild 196: SSH-Verbindung: Anmelden beim Remote Manager

► Geben Sie Benutzerkennung und Kennwort ein und bestätigen Sie Ihre Eingaben durch Klicken auf die Schaltfläche *Login*.

Anschließend wird das Hauptmenü des Remote Manager angezeigt (siehe Bild 198 auf Seite 331).

– *Einloggen beim Remote Manager über eine Telnet-Verbindung*

Es wird das Anmelde-Fenster des Remote Manager angezeigt:

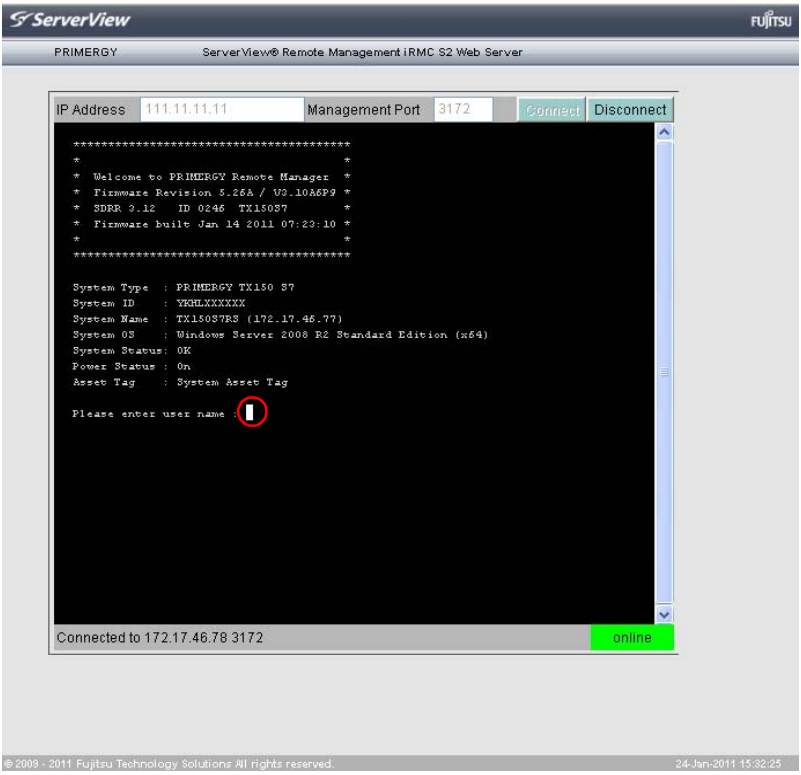


Bild 197: Telnet-Verbindung: Anmelden beim Remote Manager

Je nachdem, ob ServerView-Agenten auf dem System schon einmal gestartet wurden, wird das Anmelde-Fenster mit oder ohne Systeminformationen angezeigt (siehe Seite 338).

► Geben Sie Benutzerkennung und Kennwort ein und bestätigen Sie Ihre Eingaben durch Drücken der Taste Enter.

Anschließend wird das Hauptmenü des Remote Manager angezeigt (siehe Bild 198 auf Seite 331).

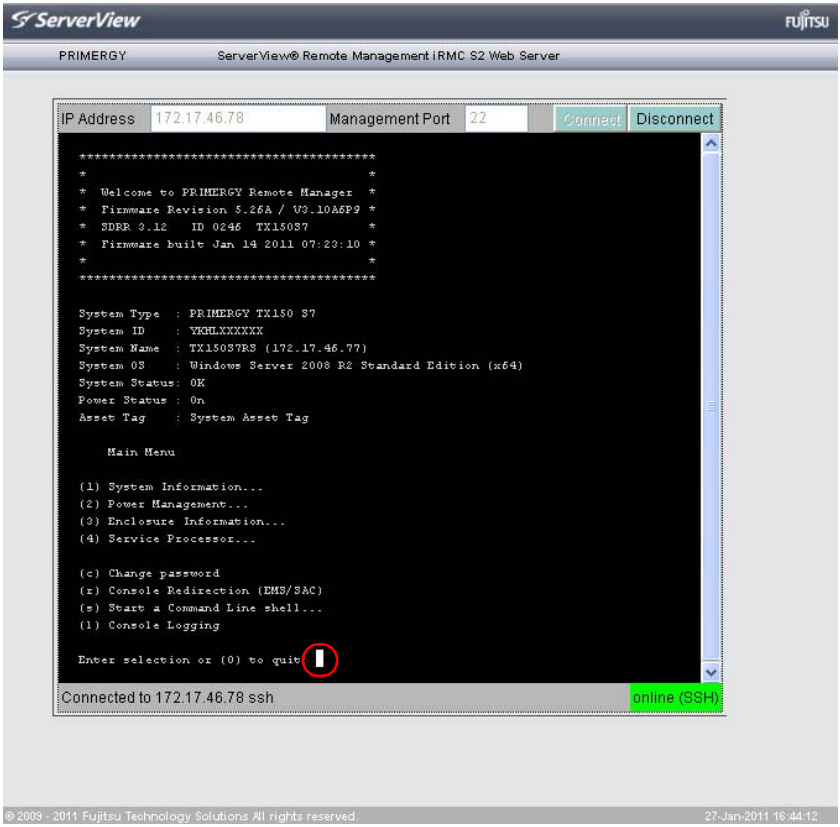


Bild 198: Hauptmenü des Remote Manager

Telnet /SSH-Verbindung beenden

- Die Verbindung zum Remote Manager beenden Sie durch Klicken auf die Schaltfläche *Disconnect* in der Verbindungsleiste des Remote Manager-Fensters oder indem Sie im Hauptmenü des Remote Manager auf die Taste 0 drücken (siehe Bild 198).

8 iRMC S2/S3 über Telnet/SSH (Remote Manager)

Für den iRMC S2/S3 gibt es eine Telnet-basierte Oberfläche - den so genannten Remote Manager. Den Remote Manager können Sie über folgende Schnittstellen aufrufen:

– iRMC S2/S3 -Web-Oberfläche (siehe Seite 326)
– beliebiger Telnet/SSH-Client
– ServerView Remote Management Frontend

Der iRMC S2/S3 unterstützt gesicherte Verbindungen über SSH (**S**ecure **Sh**ell). Die Oberfläche des Remote Manager ist für Telnet und SSH-Verbindungen identisch. Im Prinzip kann jeder Telnet/SSH-Client, der VT100-Sequenzen versteht, für den Zugriff auf den iRMC S2/S3 verwendet werden. Es wird jedoch empfohlen, die iRMC S2/S3 -Web-Oberfläche oder das ServerView Remote Management Frontend (im Folgenden kurz: Remote Management Frontend) zu verwenden.

Maximale Anzahl paralleler Sitzungen:

– Telnet: maximal 4
– SSH: maximal 4
– Telnet und SSH insgesamt: maximal 4

Im diesem Kapitel sind Bedienung und Funktionen des iRMC S2/S3 über den Remote Manager im Einzelnen beschrieben. Am Ende des Kapitels finden Sie außerdem einen kurzen Überblick über SMASH CLP.

8.1 Voraussetzung am verwalteten Server

Für den iRMC S2/S3 muss der Zugriff über Telnet aktiviert sein (siehe Abschnitt "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 252).

Der Zugang über das Telnet-Protokoll ist aus Sicherheitsgründen standardmäßig deaktiviert, da Passwörter im Klartext übertragen werden.

Da der ServerView Operations Manager den Wert des Management-Ports nicht kennt, arbeitet das Remote Management Frontend mit dem Default-Wert.

Da nach dem Start des Remote Management Frontends nicht automatisch eine Verbindung aufgebaut wird, können Sie einen vom Default-Wert abweichenden Wert für den Management-Port auch noch nach dem Start des Remote Management Frontends korrigieren.

8.2 Remote Manager bedienen

Anhand von Bild 199, das einen Ausschnitt aus dem Hauptmenü des Remote Manager zeigt, ist nachfolgend die Bedienung des Remote Manager exemplarisch dargestellt.

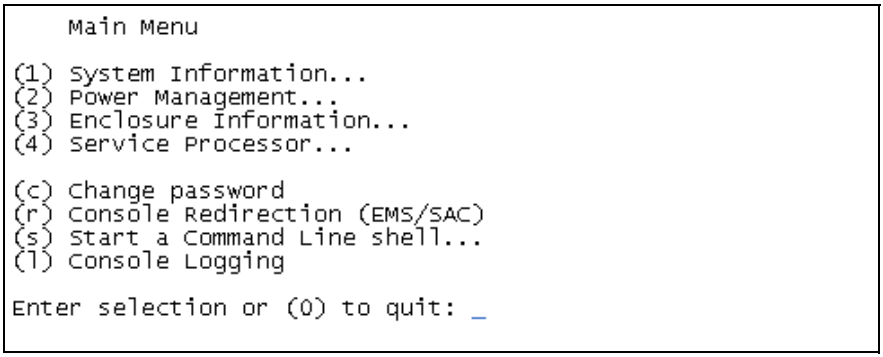


Bild 199: Bedienung des Remote Manager

- Den gewünschten Menüpunkt wählen Sie aus, indem Sie die Ziffer / den Buchstaben eingeben, der diesem Menüpunkt vorangestellt ist (z.B. „c“ für Change password).

  Funktionen, die einem Benutzer nicht erlaubt sind, sind mit einem Gedankenstrich (-) gekennzeichnet, Funktionen, die nicht verfügbar sind, mit einem Stern (*).

- Mit der Taste 0 oder der Tastenkombination Ctrl D beenden Sie den Remote Manager. Es wird ein entsprechendes Ereignis in das Eventlog geschrieben.

8.3 Menü-Übersicht

Das Remote Manager Menü für den iRMC S2/S3 ist wie folgt strukturiert:

- **System Information**
  - View Chassis Information
  - View Mainboard Information
  - View OS and SNMP Information
  - Set ASSET Tag
- **Power Management**
  - Immediate Power Off
  - Immediate Reset
  - Power Cycle
  - Power On
  - Graceful Power Off (Shutdown)
  - Graceful Reset (Reboot)
  - Raise NMI (via iRMC S2/S3)
- **Enclosure Information**
  - System Event-Log
    - View Systeme Eventlog (text, newest first)
    - View System Eventlog (text, oldest first)
    - Dump System Eventlog (raw, newest first)
    - Dump System Eventlog (raw, oldest first)
    - View System Eventlog Information
    - Clear System Eventlog

  - Internal Eventlog
    - View Internal Eventlog (text, newest last)
    - Dump Internal Eventlog (raw, newest last)
    - View Internal Eventlog Information
    - Clear Internal Eventlog
    - Change Internal Eventlog mode
  - Temperature
  - Voltages/Current
  - Fans
  - Power Supplies
  - Memory Sensor
  - Door Lock
  - CPU Sensors
  - Component Status (Lightpath)
  - List All Sensors
- **Service Processor**
  - Configure IP Parameters
  - List IP Parameters
  - Toggle Identify LED
  - Reset iRMC S2/S3 (Warm reset)
  - Reset iRMC S2/S3 (Cold reset)
- **Change password**
- **Console Redirection (EMS/SAC)**
- **Start a Command Line shell**
- **Console Logging**

8.4 Anmeldeprozess

Sobald eine Verbindung zum iRMC S2/S3 aufgebaut ist, wird im Terminal Client am Remote-Arbeitsplatz das Anmelde-Fenster des Remote Managers (Telnet/SSH-Fenster) angezeigt.

Je nachdem, ob ServerView-Agenten auf dem System schon einmal gestartet wurden, wird das Anmelde-Fenster mit oder ohne Systeminformationen angezeigt.

Beim Anmelden über eine SSH-Verbindung: Falls der Host-Key des verwalteten Servers noch nicht am Remote-Arbeitsplatz registriert ist, meldet der SSH-Client einen Security-Alert mit Vorschlägen für das weitere Vorgehen.

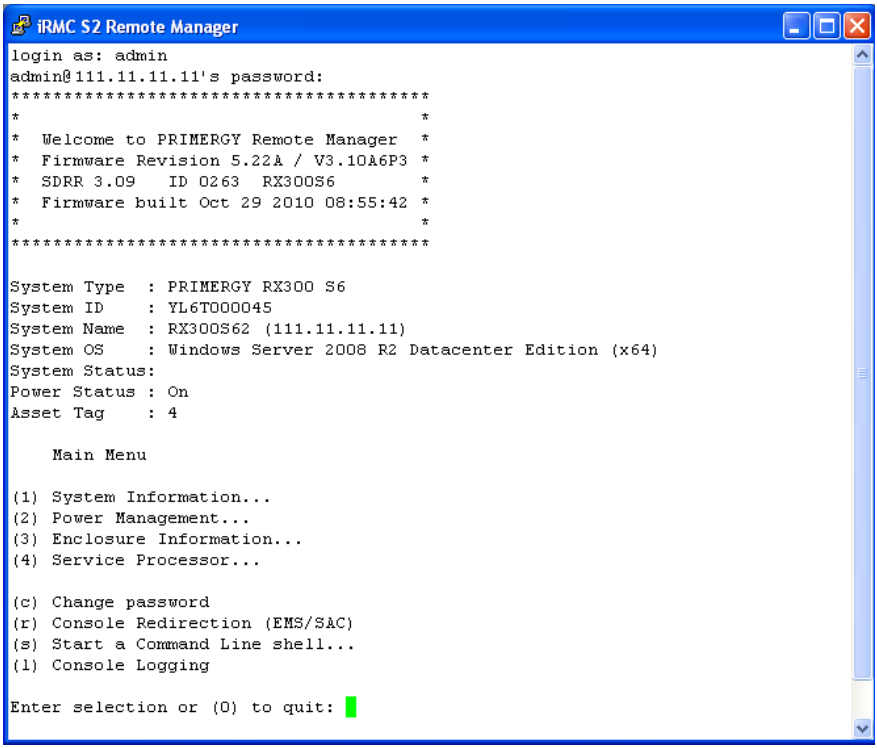

iRMC S2 Remote Manager
login as: admin
admin@111.11.11.11's password:
Welcome to PRIMERGY Remote Manager
Firmware Revision 5.22A / V3.10A6P3
SDRR 3.09 ID 0263 RX300S6
Firmware built Oct 29 2010 08:55:42
System Type : PRIMERGY RX300 S6
System ID : YL6T000045
System Name : RX300S62 (111.11.11.11)
System OS : Windows Server 2008 R2 Datacenter Edition (x64)
System Status:
Power Status : On
Asset Tag : 4
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging
Enter selection or (0) to quit:

Bild 200: Remote Manager: Anmelde-Fenster (mit Systeminformation)

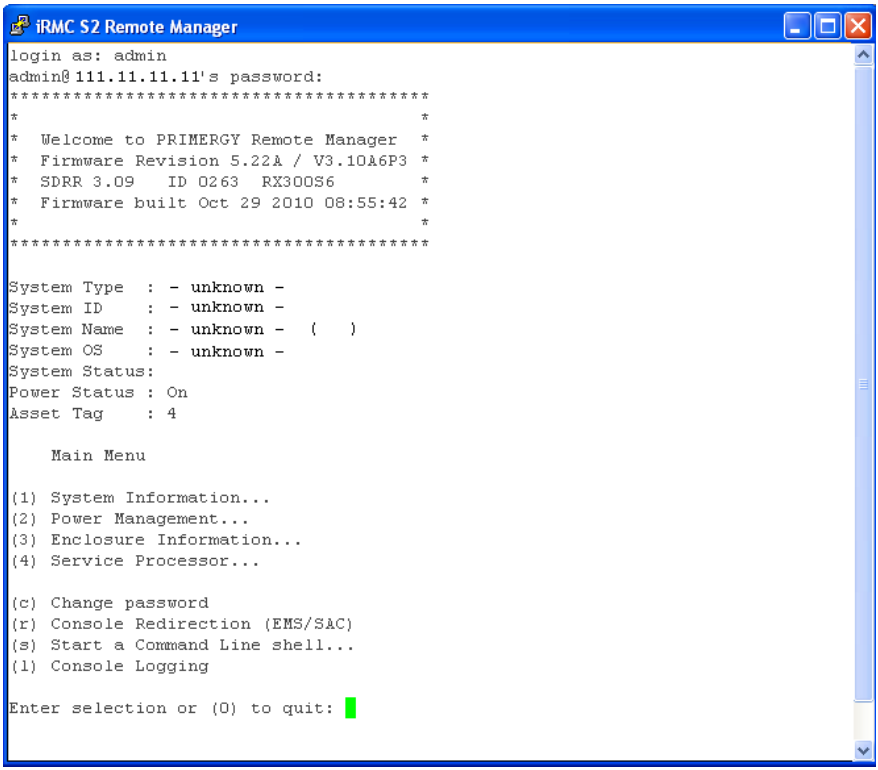

iRMC S2 Remote Manager
login as: admin
admin@111.11.11.11's password:
****
*   *
* Welcome to PRIMERGY Remote Manager   *
* Firmware Revision 5.22A / V3.10A6P3 *
* SDRR 3.09   ID 0263   RX300S6   *
* Firmware built Oct 29 2010 08:55:42 *
*   *
****
System Type   : - unknown -
System ID   : - unknown -
System Name   : - unknown -   (   )
System OS   : - unknown -
System Status:
Power Status : On
Asset Tag   : 4
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging
Enter selection or (0) to quit:

Bild 201: Remote Manager: Anmelde-Fenster (ohne Systeminformation)

Im Remote Manager-Fenster erhalten Sie Informationen zu dem betreffenden Server, anhand derer er sich identifizieren lässt, und zum Betriebszustand des Servers (Power Status). Einige Angaben (z. B. der System Name) werden nur für Server angezeigt und nur dann, wenn der Server entsprechend konfiguriert ist.

- ► Um den Remote Manager zu nutzen, müssen Sie sich mit einer Benutzerkennung und einem Passwort anmelden.

  Anschließend wird ein entsprechendes Ereignis in das Eventlog geschrieben und das entsprechende Hauptmenü des Remote Manager angezeigt (siehe Abschnitt "Hauptmenü des Remote Manager" auf Seite 340).

  Sie können den Anmeldevorgang vorzeitig mit Ctrl D beenden.

8.5 Hauptmenü des Remote Manager

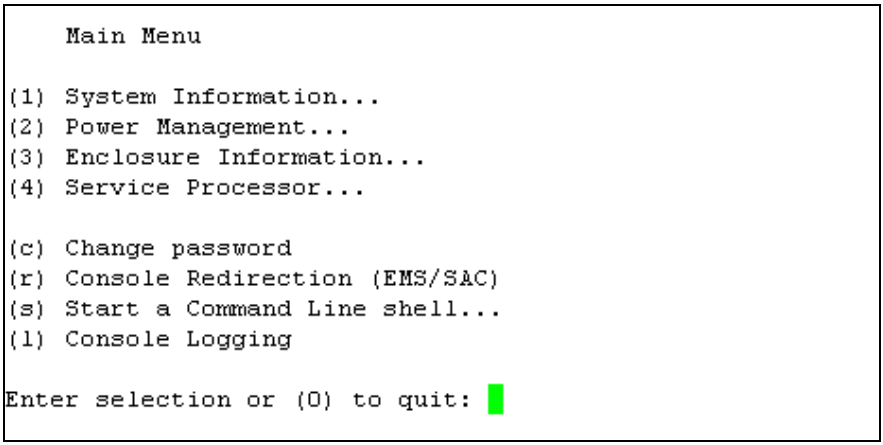


Bild 202: Remote Manager: Hauptmenü-Fenster

Das Hauptmenü des Remote Manager bietet Ihnen folgende Funktionen:

System Information...	Informationen zum verwalteten Server einsehen und den Asset Tag (Bestandskennzeichen) setzen (siehe Abschnitt "System Information - Informationen zum verwalteten Server" auf Seite 344).
Power Management...	Server ein/ausschalten (siehe Abschnitt "Power Management" auf Seite 345).
Enclosure Information...	Informationen über den aktuellen Systemzustand anfordern, z. B. Fehler- und Ereignismeldungen von Error-Log und Eventlog überprüfen (Temperatur, Lüfter, ...) (siehe Abschnitt "Enclosure Information - System / interner Eventlog, Status der Sensoren" auf Seite 346).

Tabelle 8: Hauptmenü des Remote Manager

Service Processor...	Den iRMC S2/S3 konfigurieren (z.B. Firmware aktualisieren oder IP-Adresse ändern) (siehe Abschnitt "Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S2" auf Seite 350).
Change password	Passwortwort ändern (siehe Abschnitt "Passwort ändern" auf Seite 344).
Console Redirection (EMS/SAC)	Text-Konsolen-Umleitung (siehe Abschnitt "Console Redirection (EMS/SAC) - Text-Konsolen-Umleitung starten" auf Seite 351)
Start a Command Line shell...	Command Line Shell starten (siehe Abschnitt "Start a Command Line shell... - SMASH CLP Shell starten" auf Seite 351).
Console Logging	Meldungsausgabe auf die Text-Konsole steuern (siehe Abschnitt "Console Logging - Meldungsausgabe auf die Text-Konsole (seriell)" auf Seite 353).

Tabelle 8: Hauptmenü des Remote Manager

8.6 Erforderliche Benutzerberechtigungen

Tabelle 9 gibt einen Überblick, welche Benutzerberechtigungen zur Nutzung der einzelnen Funktionen des Remote Manager erforderlich sind.

Menüpunkte des Remote Manager	Zulässig mit IPMI Privilege Level				Erforderliche Berechtigung			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
System Information...	X	X	X	X				
View Chassis / M ainboard, / OS Information						X		
Set ASSET Tag[1)]						X		
Set System Name [1)]						X		
Set System Operating System Information[1)]						X		
Set System Description[1)]						X		
Set System Location Information (SNMP)[1)]						X		
Set System Contact Information (SNMP)[1)]						X		
Power Management..	X	X	X					
Ansehen *Enclosure Information*	X	X	X	X				
System Eventlog - View/Dump System Eventlog	X	X	X	X				
System Eventlog - Clear System Eventlog	X	X	X					
Internal Eventlog - View/Dump Internal Eventlog	X	X	X	X				
Internal Eventlog - Clear Internal Eventlog	X	X	X	X				
Sensor-Übersichten (*Temperature*, *Fans* ...)	X	X	X	X				

Tabelle 9: Berechtigungen zur Nutzung des Remote Manager-Menüs

Menüpunkte des Remote Manager	Zulässig mit IPMI Privilege Level				Erforderliche Berechtigung			
	OEM	Administrator	Operator	User	Benutzerkonfiguration erlaubt	iRMC S2/S3 Konfiguration erlaubt	Konsolenumleitung erlaubt	Remote Storage erlaubt
Ansehen *Service Processor...*	X	X	X	X				
Service Processor... - List IP Parameters						X		
Service Processor... - Configure IP Parameters						X		
Service Processor... - Toggle Identify LED	X	X	X	X				
Service Proc. ... - Reset iRMC S2/S3 (warm/cold reset)	X	X				X		
Change Password					X			
Console Redirection (EMS/SAC)	X	X	X					
Start a command Line shell...	X	X	X	X				
Console Logging	X	X	X					

Die Aktion ist nur möglich, wenn keine ServerView-Agenten gestartet sind

Tabelle 9: Berechtigungen zur Nutzung des Remote Manager-Menüs

8.7 Passwort ändern

Mit dem Menüpunkt *Change password* kann ein Benutzer mit der Berechtigung *Benutzerkonfiguration erlaubt* (siehe Seite 72) sein eigenes Passwort sowie die Passwörter anderer Benutzer ändern.

8.8 System Information - Informationen zum verwalteten Server

Wenn Sie im Hauptmenü den Menüpunkt *System Information...* auswählen, erhalten Sie das folgende Menü:

```
    System Information Menu

(1) View Chassis Information
(2) View Mainboard Information
(3) View OS and SNMP Information

(4) Set ASSET Tag
(*) Set System Name
(*) Set System Operating System Information
(*) Set System Description
(*) Set System Location Information (SNMP)
(*) Set System Contact Information (SNMP)

Enter selection or (0) to quit:
```

Bild 203: Remote Manager: System Information-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

View Chassis Information	Informationen über das Gehäuse des verwalteten Servers und seine Produktdaten.
View *Mainboard Information*	Informationen zur Systembaugruppe des verwalteten Servers und ihren Produktdaten.
View *OS and SNMP Information*	Informationen zum Betriebssystem und zur ServerView-Version des verwalteten Servers und zu den SNMP-Einstellungen.
Set ASSET Tag	Kundenspezifischen Asset-Tag für den verwalteten Server setzen.

Tabelle 10: Menü System Information

8.9 Power Management

Wenn Sie im Hauptmenü den Menüpunkt *Power Management...* auswählen, erhalten Sie das folgende Menü:

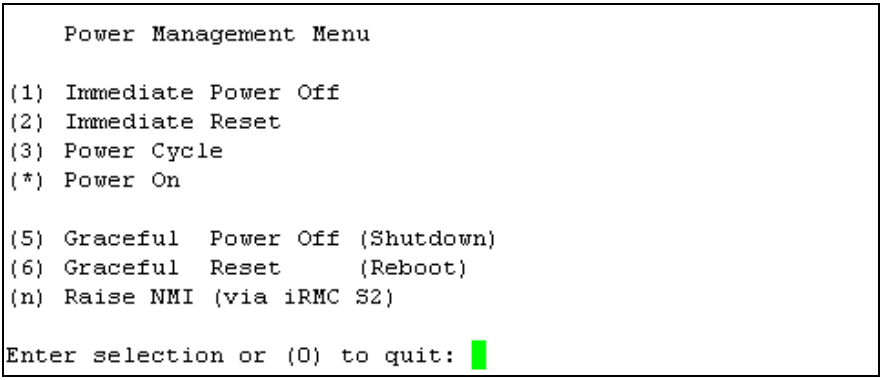

Power Management Menu
(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On
(5) Graceful Power Off (Shutdown)
(6) Graceful Reset (Reboot)
(n) Raise NMI (via iRMC S2)
Enter selection or (0) to quit:

Bild 204: Remote Manager: Power Management-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

Immediate Power Off	Schaltet den Server unabhängig vom Status des Betriebssystems aus.
Immediate Reset	Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).
Power Cycle	Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein.
Power On	Schaltet den Server ein.
Graceful Power Off (Shutdown)	Graceful Shutdown und Power Off. Der Menüpunkt ist nur verfügbar, wenn ServerView-Agenten installiert und beim iRMC S2/S3 als „connected“ gemeldet sind.
Graceful Reset (Reboot)	Graceful Shutdown und Reboot. Der Menüpunkt ist nur verfügbar, wenn ServerView-Agenten installiert und beim iRMC S2/S3 als „connected“ gemeldet sind.
Raise NMI (via iRMC S2/S3)	Löst eine nicht-maskierbare Unterbrecheung (non-askable interrupt, NMI) via iRMC S2/S3 aus.

Tabelle 11: Menü Power Management

8.10 Enclosure Information - System / interner Eventlog, Status der Sensoren

Wenn Sie im Hauptmenü den Menüpunkt *Enclosure Information...* auswählen, erhalten Sie das folgende Menü:

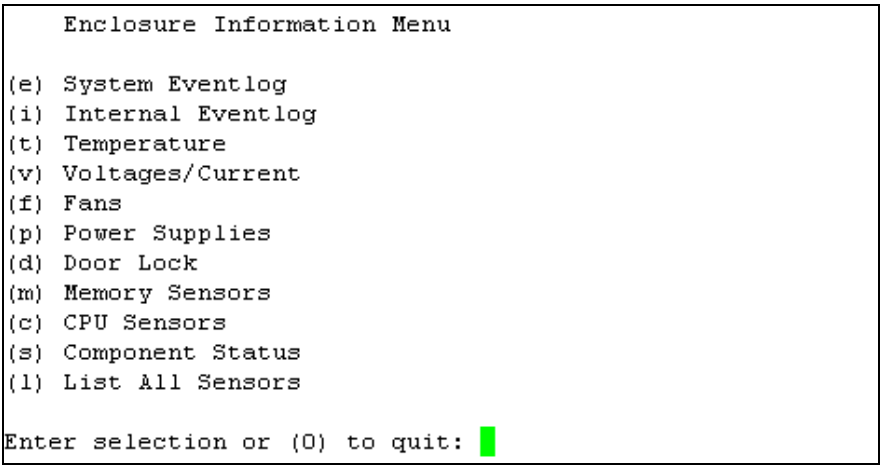


Bild 205: Remote Manager: Enclosure Information-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

System Eventlog	Ruft das Menü *System Eventlog* auf (siehe Abschnitt "System Event-Log" auf Seite 348).
Internal Eventlog	Ruft das Menü *Internal Eventlog* auf (siehe Abschnitt "Internal Eventlog" auf Seite 349).
Temperature	Informationen über die Temperatur-Sensoren und deren Status anzeigen.
Voltages/Current	Informationen über die Spannungs- und Strom-Sensoren und deren Status anzeigen.
Fans	Informationen über die Lüfter und deren Status anzeigen.
Power Supplies	Informationen über die Netzteile und deren Redundanz-Status anzeigen.
Door Lock	Informationen anzeigen, ob Front oder Gehäuse geöffnet sind.
Memory Sensors	Informationen zu den Status der Speichersensoren anzeigen.
CPU Sensors	Prozessor(en) des Servers lokalisieren.
Component Status	Detail-Informationen zu allen Sensoren anzeigen, die über eine PRIMERGY Diagnostic LED verfügen.
List all Sensors	Detail-Informationen zu allen Sensoren anzeigen.

Tabelle 12: Menü Enclosure Information

System Event-Log

Wenn Sie im Untermenü *Enclosure Information...* den Menüpunkt *System Eventlog* auswählen, erhalten Sie das folgende Menü:

```
    System Eventlog Menu

(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)

(5) View System Eventlog Information
(6) Clear System Eventlog

Enter selection or (0) to quit:
```

Bild 206: Remote Manager: System Eventlog-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

View System Eventlog (text, newest first)	Der Inhalt des Fehlerspeichers (System Eventlog) wird in lesbarer Form und chronologischer Reihenfolge am Bildschirm ausgegeben (der jüngste Eintrag zuerst).
View System Eventlog (text, oldest first)	Der Inhalt des Fehlerspeichers wird in lesbarer Form und umgekehrter chronologischer Reihenfolge am Bildschirm ausgegeben (der älteste Eintrag zuerst).
Dump System Eventlog (raw, newest first)	Der Inhalt des Fehlerspeichers wird in chronologischer Reihenfolge ausgeschrieben (der jüngste Eintrag zuerst).
Dump System Eventlog (raw, oldest first)	Der Inhalt des Fehlerspeichers wird in umgekehrt chronologischer Reihenfolge ausgeschrieben (der älteste Eintrag zuerst).
View System Eventlog Information	Informationen zum Fehlerspeicher.
Clear System Eventlog	Der Inhalt des Fehlerspeichers wird gelöscht.
Change System Eventlog mode	Ändert den Puffer-Modus des Fehlerspeichers vom Modus *Ring Buffer* in den Modus *Linear Buffer* und umgekehrt.

Tabelle 13: Menü System Eventlog

Internal Eventlog

Wenn Sie im Untermenü *Enclosure Information...* den Menüpunkt *Internal Eventlog* auswählen, erhalten Sie das folgende Menü:

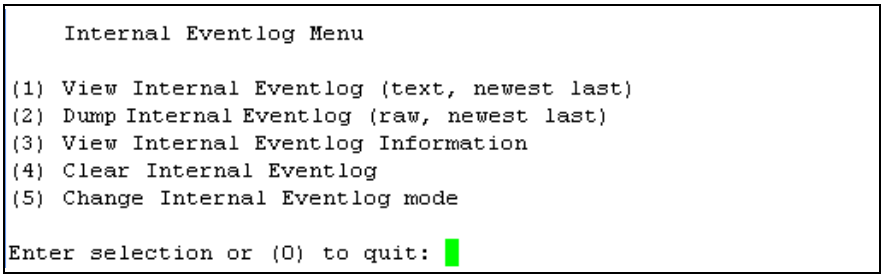

Internal Eventlog Menu
(1) View Internal Eventlog (text, newest last)
(2) Dump Internal Eventlog (raw, newest last)
(3) View Internal Eventlog Information
(4) Clear Internal Eventlog
(5) Change Internal Eventlog mode
Enter selection or (0) to quit:

Bild 207: Remote Manager: Menü Internal Eventlog

Das Untermenü bietet Ihnen folgende Funktionen:

View Internal Eventlog (text, newest last)	Der Inhalt des internen Ereignisspeichers (internal Eventlog) wird in lesbarer Form und umgekehrter chronologischer Reihenfolge am Bildschirm ausgegeben (der neueste Eintrag zuletzt).
Dump Internal Eventlog (raw, newest last)	Der Inhalt des internen Ereignisspeichers wird in umgekehrt chronologischer Reihenfolge am Bildschirm ausgegeben (der neueste Eintrag
View Internal Eventlog Information	Informationen zum internen Ereignisspeicher.
Clear Internal Eventlog	Inhalt des internen Ereignisspeichers wird gelöscht.
Change Internal Eventlog mode	Ändert den Puffer-Modus des internen Ereignisspeichers vom Modus *Ring Buffer* in den Modus *Linear Buffer* und umgekehrt.

Tabelle 14: Menü Internal Eventlog

8.11 Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S2

Wenn Sie im Hauptmenü den Menüpunkt *Service Processor...* auswählen, erhalten Sie das folgende Menü:

```
    Service Processor Menu

(1) Configure IP Parameters
(2) List IP Parameters

(3) Toggle Identify LED

(4) Reset iRMC S2 (Warm reset)
(5) Reset iRMC S2 (Cold reset)

Enter selection or (0) to quit:
```

Bild 208: Remote Manager: Service Processor-Fenster

Das Untermenü bietet Ihnen folgende Funktionen:

Es wird empfohlen, nach einem *Reset iRMC S2/S3 (Cold Reset)* oder *Reset iRMC S2/S3 (Warm Reset)* den Server neu zu starten (siehe Seite 196).

Configure IP Parameters	IPv4 / IPv6-Adressen des iRMC S2/S3 konfigurieren. Zu Details für die Einzelnen Einstellungen siehe Abschnitt "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 252).
List IP Parameters	IP-Einstellungen anzeigen.
Toggle Identify LED	PRIMERGY Identifizierungs-LED ein-/ausschalten.
Reset iRMC S2/S3 (Warm reset)	Reset des iRMC S2/S3 durchführen. Die Verbindung wird beendet. Es werden nur die Schnittstellen neu initialisiert.

Tabelle 15: Menü Service Processor

Reset iRMC S2/S3 (Cold reset)	Reset des iRMC S2/S3 durchführen. Die Verbindung wird beendet. Der iRMC S2/S3 wird komplett neu initialisiert.

Tabelle 15: Menü Service Processor

8.12 Console Redirection (EMS/SAC) - Text-Konsolen-Umleitung starten

Unter dem Menüpunkt *Console Redirection (EMS/SAC)* des Hauptmenüs können Sie die Text-Konsolen-Umleitung starten.

Die Text basierte Console Redirection funktioniert via LAN nur mit Serial 1.

Falls die Console Redirection auch bei laufendem Betriebssystem genutzt werden soll, muss der *Serial 1Multiplexer* auf *System* konfiguriert sein.

Zum Verlassen der Text-Konsole verwenden Sie die Tastenkombinationen „<ESC>(“ oder „~.“ (tilde dot).

Je nach Typ des PRIMERGY Servers funktioniert unter Umständen nur eine dieser beiden Möglichkeiten.

8.13 Start a Command Line shell... - SMASH CLP Shell starten

Unter dem Menüpunkt *Start a Command Line shell...* des Hauptmenüs können Sie eine SMASH CLP Shell starten. SMASH CLP ist die Abkürzung für „**S**ystems **M**anagement **A**rchitecture“ for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol“. Dieses Protokoll ermöglicht eine Verbindung zwischen der Management- Station und dem verwalteten Server auf Basis von Telnet oder SSH. Näheres zu SMASH CLP finden Sie im Abschnitt "Command Line Protocol (CLP)" auf Seite 355.

Wenn Sie im Hauptmenü den Menüpunkt *(s) Start a Command Line shell...* auswählen, wird das folgende Fenster angezeigt:

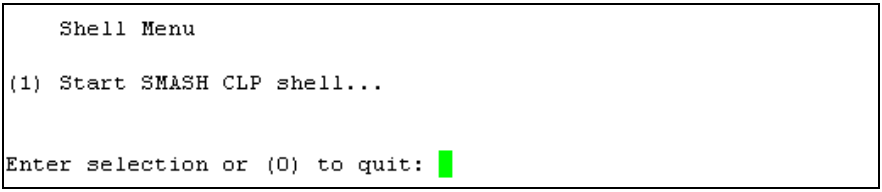


Bild 209: Remote Manager: Start a SMASH CLP shell...-Fenster

- Wählen Sie *(1) Start a SMASH CLP shell...*, um die SMASH CLP Shell zu starten.

8.14 Console Logging - Meldungsausgabe auf die Text-Konsole (seriell)

Unter dem Menüpunkt *Console Logging* des Hauptmenüs können Sie die Meldungsausgabe (Logging) auf die Text-Konsole (serielle Schnittstelle) steuern.

Wenn Sie im Hauptmenü den Menüpunkt *(l) Console Logging* auswählen, wird das folgende Fenster angezeigt:

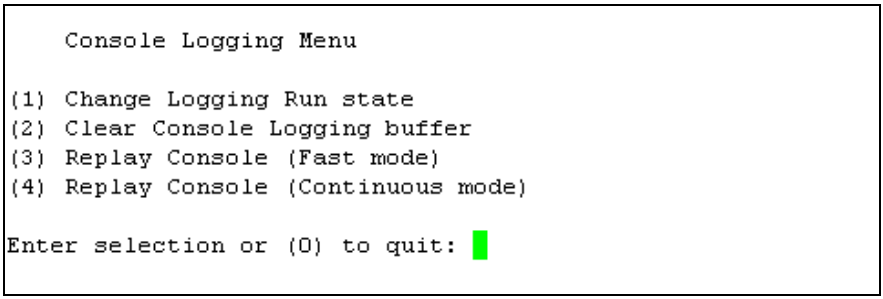

Console Logging Menu
(1) Change Logging Run state
(2) Clear Console Logging buffer
(3) Replay Console (Fast mode)
(4) Replay Console (Continuous mode)
Enter selection or (0) to quit:

Bild 210: Remote Manager: Console Logging

Das Untermenü bietet Ihnen folgende Funktionen:

Change Logging Run State	Ausführungsstatus des Console Logging anzeigen und steuern. Näheres siehe "Console Logging Run State Menu" auf Seite 354
Clear Console Logging buffer	Console Logging-Puffer löschen.
Replay Console (Fast mode)	Console Logging anzeigen (Schnellmodus)
Replay Console (Continuous mode)	Console Logging anzeigen (kontinuierlicher Modus)

Tabelle 16: Menü Console Logging

Console Logging Run State Menu

```
    Console Logging Run State Menu
    State: STOPPED (Normal Mode)

(r) Start Console Logging
(*) Stop Console Logging

(t) Toggle to Text Mode
(*) Toggle to Normal Mode

Enter selection or (0) to quit:
```

Bild 211: Remote Manager: Console Logging Run State Menu

Das *Console Logging Run State Menu* bietet Ihnen folgende Funktionen:

Start Console Logging	Logging auf die Text-Konsole starten.
Stop Console Logging	Logging auf die Text-Konsole stoppen.
Toggle to Text Mode	In den Text-Modus schalten. Im Text-Modus werden vor der Ausgabe auf Konsole alle Escape-Sequenzen herausgefiltert.
Toggle to Normal Mode	In den Normal-Modus schalten. Im Normal-Modus werden vor der Ausgabe auf Konsole nur die folgenden Escape-Sequenzen herausgefiltert: <ESC>(<ESC>stop <ESC>Q <ESC>R<ESC>r<ESC>R <ESC>^ Damit ist in eingeschränktem Umfang auch Farbe, Pseudo-Grafik etc. darstellbar.

Tabelle 17: Menü Console Logging Run State

8.15 Command Line Protocol (CLP)

Der iRMC S2/S3 unterstützt verschiedene Text-basierte Benutzerschnittstellen, so genannte Benutzer-Shells, die für die einzelnen Benutzer unterschiedlich konfiguriert werden können.

Die Initiative **S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware (SMASH) definiert eine Reihe von Spezifikationen mit folgenden Zielen:

– Bereitstellung standardisierter Schnittstellen für das Management heterogener Rechnerlandschaften.

– Bereitstellung eines Architektur-Framework mit einheitlichen Schnittstellen, Hardware- und Software-Erkennung, Resource Addressing und Datenmodellen.

Weitere Informationen über SMASH finden unter folgendem Link:

http://www.dmtf.org/standards/smash

SMASH CLP-Syntax

SMASH CLP spezifiziert eine allgemeine Kommandozeilen-Syntax und Meldungsprotokoll-Semantik für das Management von Rechnern im Internet sowie im Umfeld von Unternehmen und Service Providern. Detaillierte Informationen zum SMASH CLP finden Sie in dem DMTF Dokument „Server Management Command Line Protocol Specification (SM CLP)DSP0214“.

Die allgemeine Syntax des CLP lautet wie folgt:

```
<verb> [<options>] [<target>] [<properties>]
```

<verb>

Verben spezifizieren, welches Kommando oder welche Aktion auszuführen ist. Die Liste der Verben beschreibt z. B. folgende Tätigkeiten:

– Daten generieren (*set*) und wiedergewinnen (*show*)

– Status eines Ziels ändern (*reset*, *start*, *stop*)

– aktuelle Sitzung steuern (*cd*, *version*, *exit*)

– Informationen zu Kommandos liefern (*help*)

In iRMC S2/S3 -Systemen ermöglicht außerdem das Verb *oemfujitsu* die Nutzung spezieller OEM-Kommandos.

<options>

(Kommando-)Options legen die Einzelheiten zur Aktion oder zum Verhalten eines Verbs fest. Options dürfen in einer Kommandozeile unmittelbar hinter dem Verb stehen und müssen immer mit einem vorangehenden Bindestrich („-“) angegeben werden.

Mithilfe von Options können Sie z.B.

- das Ausgabeformat festlegen,
- die rekursive Ausführung des Kommandos zulassen,
- die Version des Kommandos anzeigen lassen oder
- Hilfe-Informationen anfordern.

<target>

<target> spezifiziert die Adresse oder den Pfad des von dem Kommando zu manipulierenden Objekts, d.h. des Kommandoziels. Dies kann ein einzelnes überwachtes Element (Managed Element) sein, wie z.B. eine Festplatte, eine Netzkarte (Network Interface Card, NIC), oder das Administrationsprogramm (Management Assistance Program, MAP) selbst. Als mögliches Ziel kommen aber u.a. auch Services infrage, wie beispielsweise ein Transport-Service.

Unter einem <target> lassen sich mehrere Managed Elements zusammenfassen, deren Verwaltung vom Administrationsprogramm unterstützt wird, z.B. das System als Ganzes.

Pro Kommando darf nur ein einziges <target> angegeben werden.

<properties>

<properties> beschreiben die Eigenschaften des Kommandoziels, die zur Ausführung des Kommandos erforderlich sind. So identifizieren die <properties> über die Klasse des Kommandoziels die Properties im Zielobjekt, deren Werte vom Kommando ermittelt oder modifiziert werden.

Benutzerdaten im CLP (Überblick)

Die Daten innerhalb des CLP sind hierarchisch angeordnet. Mithilfe des Kommandos *cd* können Sie innerhalb dieser Struktur navigieren.

Bild 212 gibt einen Überblick über die Benutzerdaten im CLP. Die Namen in den Rechtecken bezeichnen Kommandoziele. Auf jeder Ebene der Hierarchie zeigt das Kommando bzw. Verb *show* die verfügbaren Ziele (Targets), Properties und Verben an.

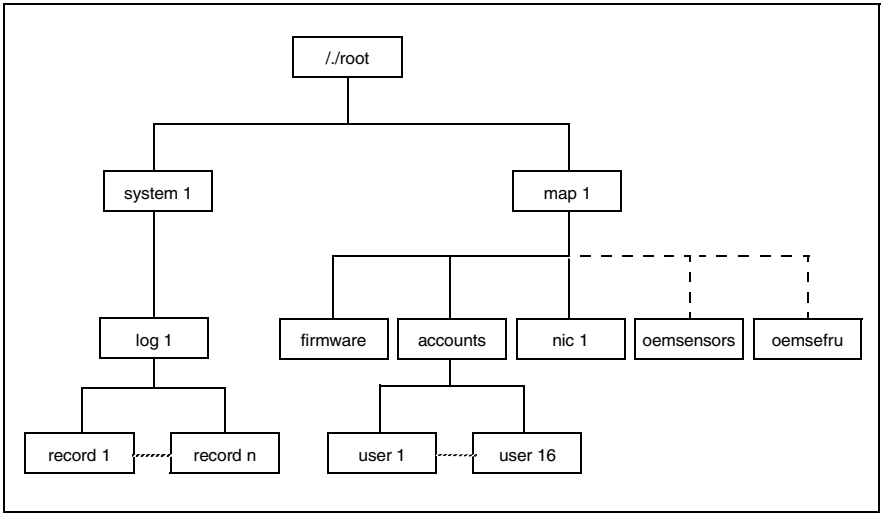


Bild 212: Struktur der Benutzerdaten in SMASH CLP

Hierarchie der CLP-Kommandos

Tabelle 18 auf Seite 358 gibt einen Überblick über die Hierarchie der CLP-Kommandos.

Verb / Target	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
/./		Root	X	X	X	X	X						
system1 **map1**													
system1	name enabledstate	Host System	X	X	X	X	X		System	PON	POFF		
...log1		Event Log (SEL)	X	X	X	X	X		iRMC				X
....record<n>	number date time sensordescription eventdescription eventdirection	Single SEL entry	X	X	X	X	X		iRMC				X
map1	name	iRMC	X	X	X	X	X		iRMC				X
...firmware	version	iRMC FW	X	X	X	X	X		iRMC			X	X
...accounts		Accounts	X	X	X	X	X	X	iRMC				X
.....user<n>	username password group	User	X	X	X	X	X	X	iRMC				X
...nic1	networkaddress oemfsc_nonvol_networkaddress oemfsc_mask oemfsc_nonvol_mask oemfsc_gateway oemfsc_nonvol_gateway oemfsc_dhcp_enable oemfsc_nonvol_dhcp_enable oemfsc_vsi_path oemfsc_vsi_server oemfsc_vsi_permission oemfsc_vsi_sustain	LAN	X	X	X	X	X	X	iRMC				X
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		iRMC				X
....oemfsc_sensor_num<n>lun<m>	oemfsc_reading oemfsc_status oemfsc_sensortype oemfsc_readingtype	Single Sensor	X	X	X	X	X		iRMC				X
...oemfsc_frus		FRU	X	X	X	X	X		iRMC				X
....oemfsc_fru_devid<n>lun<m>	oemfsc_description	Single FRU	X	X	X	X	X		iRMC				X

Tabelle 18: Hierarchie der CLP-Kommandos

9 iRMC S2/S3 via Server Configuration Manager konfigurieren

Mit dem Server Configuration Manager können Sie folgende Aufgaben durchführen:

– iRMC S2/S3 konfigurieren.

– Benutzerkennungen am iRMC S2/S3 konfigurieren und verwalten.

– Verzeichnisdienst am iRMC S2/S3 konfigurieren.

– CAS Service am iRMC S2/S3 konfigurieren.

Voraussetzung:

Auf dem verwalteten Server sind die aktuellen ServerView-Agenten installiert.

Für den Zugang zur Server Configuration Manager-Funktionalität bieten sich folgende Möglichkeiten:

– Lokal am verwalteten Server über den ServerView Installation Manager (im Folgenden kurz: Installation Manager).

– Lokal am verwalteten Windows-basierten Server über das Windows Startmenü.

  Dies wird nur für Server unterstützt, auf denen die ServerView-Agenten für Windows installiert sind.

– Am Remote-Arbeitsplatz über die grafische Oberfläche des Operations Managers.

  Dies wird nur für Server unterstützt, auf denen die ServerView-Agenten für Windows installiert sind.

Dieses Kapitel beschreibt die verschiedenen Möglichkeiten, den Server Configuration Manager aufzurufen.

Näheres zu den einzelnen Dialogen des Server Configuration Managers finden Sie in der Online-Hilfe des Server Configuration Managers.

9.1 Server Configuration Manager via ServerView Installation Manager aufrufen

Den Server Configuration Manager können Sie über den ServerView Installation Manager (im Folgenden kurz Installation Manager) aufrufen. Die Konfiguration via Installation Manager ist bei der Installation des Servers von Bedeutung. Der Installation Manager stellt den Server Configuration Manager sowohl im Rahmen der Installationsvorbereitung als auch als eigenes Wartungsprogramm zur Verfügung. Der Installation Manager ist beschrieben im Handbuch „ServerView Installation Manager“.

9.2 Server Configuration Manager über das Windows Startmenü aufrufen

Bei Windows-basierten Servern können Sie den Server Configuration Manager auch über das Windows Startmenü aufrufen.

Gehen Sie hierbei wie folgt vor:

- Wählen Sie am verwalteten Server:
  Start – All Programs – Fujitsu – ServerView – Agents – Configuration Tools – System Configuration.

  Das Fenster *System Configuration* öffnet sich:

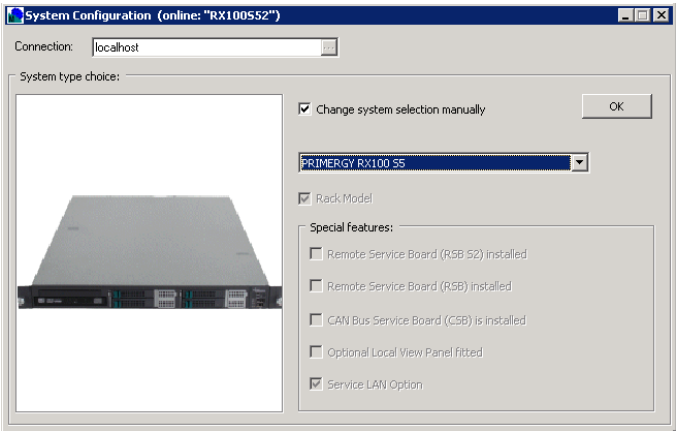


Bild 213: Fenster System Configuration

- ► Übernehmen Sie die voreingestellten Werte.
- ► Klicken Sie auf *OK*.

  Die 'Registerkarten-Ansicht' des Fensters *System Configuration* wird geöffnet.

  Durch Klicken auf die Pfeile links neben der Leiste der Reiter können Sie in der Leiste nach links bzw. rechts blättern.

Einstellungen übernehmen

Um die in den einzelnen Registerkarten vorgenommenen Einstellungen zu übernehmen, verfahren Sie pro Registerkarte wie folgt:

- ► Klicken auf die Schaltfläche *Apply*.
- ► Klicken auf die Schaltfläche *Save Page*.

  Damit die Änderungen der Einstellungen wirksam werden, bootet der iRMC S2/S3 automatisch neu.

9.3 Server Configuration Manager über den Operations Manager aufrufen

Die Server Configuration Manager-Dialoge zur Konfiguration des iRMC S2/S3 stehen Ihnen auch über die grafische Oberfläche des Operations Managers zur Verfügung. Damit können Sie den iRMC S2/S3 des verwalteten Servers vom Remote-Arbeitsplatz aus via Web-Interface konfigurieren.

Gehen Sie wie folgt vor:

- Starten Sie den Operations Manager (siehe Handbuch „ServerView Operations Manager“).

  Das Startfenster des Operation Managers wird geöffnet:

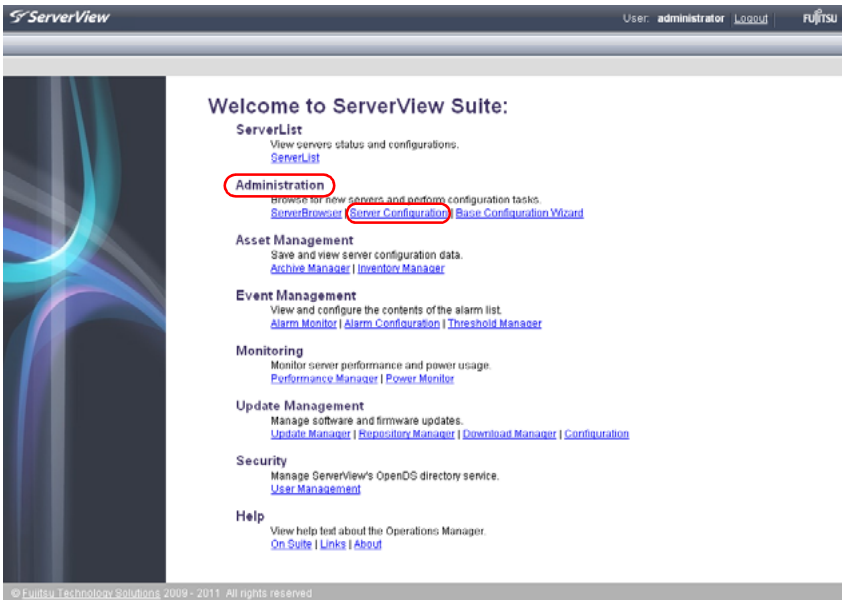

ServerView
User: administrator Logout
FUJITSU
Welcome to ServerView Suite:
ServerList
View servers status and configurations.
ServerList
Administration
Browse for new servers and perform configuration tasks.
ServerBrowser | Server Configuration | Base Configuration Wizard
Asset Management
Save and view server configuration data.
Archive Manager | Inventory Manager
Event Management
View and configure the contents of the alarm list.
Alarm Monitor | Alarm Configuration | Threshold Manager
Monitoring
Monitor server performance and power usage.
Performance Manager | Power Monitor
Update Management
Manage software and firmware updates.
Update Manager | Repository Manager | Download Manager | Configuration
Security
Manage ServerView's OpenDS directory service.
User Management
Help
View help text about the Operations Manager.
On Suite | Links | About
© Fujitsu Technology Solutions 2009 - 2011 All rights reserved

Bild 214: Operations Manager: Startfenster

► Wählen Sie im Menu des Operations Manager-Startfensters unter *Administration* den Menü-Punkt *Server Configuration*.

Das folgende Fenster wird angezeigt:

Bild 215: Operations Manager: Fenster Server Configuration - Registerkarte Server list (1)

► Klicken Sie im Strukturbaum der Registerkarte *Server list* auf den zu konfigurierenden Server.

Das folgende Fenster wird angezeigt:

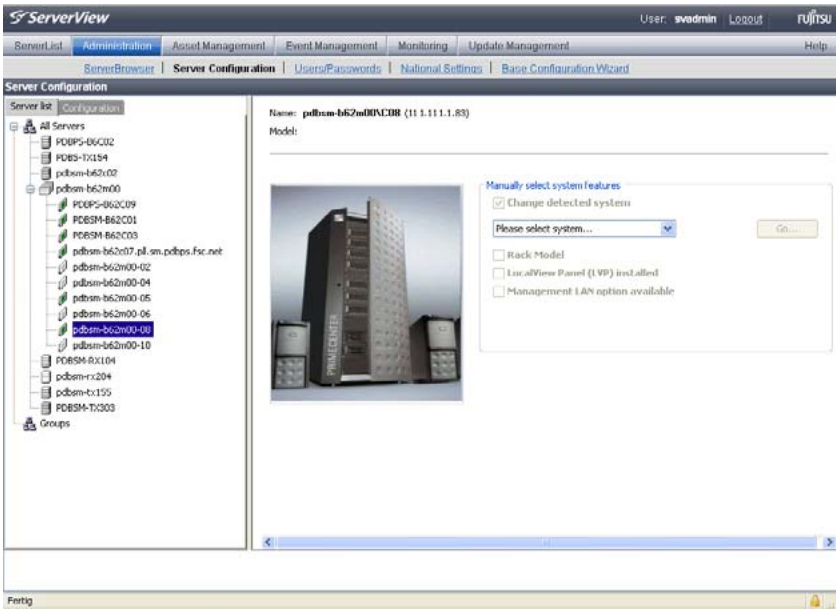


Bild 216: Operations Manager: Fenster Server Configuration - Registerkarte Server list (2)

► Spezifizieren Sie im rechten Bereich des Fensters die Details zum gewählten Server und bestätigen Sie mit *GO...* .

Der erste Dialog des Server Configuration Managers wird angezeigt.

10 Firmware aktualisieren

Dieses Kapitel informiert über folgende Themen:

– Firmware des iRMC S2/S3 (Überblick)

– Memory-Stick für die Firmware-Aktualisierung erstellen

– Firmware-Images aktualisieren

– Emergency Flash

– Flash-Tools

Die aktuellen Firmware-Versionen erhalten Sie auf der *ServerView Suite DVD 1* oder per manuellem Download aus der Download-Section des Web-Servers von Fujitsu Technology Solutions.

Die *ServerView Suite DVD 1* können Sie alle zwei Monate aktuell beziehen.

Neben der Firmware-Aktualierung besteht auch die Möglichkeit zum Firmware-Downgrade, d.h. Sie können die Firmware auf den Vorgängerstand zurücksetzen.

Bevor Sie die Firmware aktualisieren oder zurücksetzen, lesen Sie sorgfältig die mit der entsprechenden Firmware gelieferte zusätzliche Dokumentation (vor allem die Readme-Dateien).

Um die Firmware nach dem Aktualisieren / Zurücksetzen zu aktivieren, ist ein Neustart des verwalteten Servers erforderlich.

ACHTUNG!

Beachten Sie beim Aktualisieren / Zurücksetzen der Firmware, dass ein einwandfreies Funktionieren der Firmware nur dann gewährleistet ist, wenn Runtime Firmware und SDR (Sensor Data Record, siehe Seite 367) demselben Firmware Release angehören.

10.1 Firmware des iRMC S2/S3 (Überblick)

Der iRMC S2/S3 arbeitet mit zwei verschiedenen Firmware-Images. Die beiden Firmware-Images sind auf einem EEPROM (**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory) der Größe 16 MB gespeichert:

– Firmware-Image 1 (Unteres FW Image, Low FW Image)
– Firmware-Image 2 (Oberes FW Image, High FW Image)

Die Firmware des iRMC S2/S3 wird nicht im EEPROM ausgeführt, sondern wird beim Start in den SRAM-Speicher geladen und dort ausgeführt. Somit können Sie sowohl das aktive als auch das inaktive Firmware-Image online, d.h. bei laufendem Server-Betriebssystem (Windows oder Linux) aktualisieren.

Wenn beim Start der Firmware aus einem der Images ein Fehler erkannt wird, wird die Firmware automatisch aus dem anderen Image gestartet.

Aktuelle Informationen zu Firmware und EEPROM des iRMC S2/S3 erhalten Sie

– an der iRMC S2/S3-Web-Oberfläche, Seite *iRMC S2/S3 Information* (siehe Seite 171) oder
– mithilfe der Flash-Tools (siehe Seite 381).

Aktives und passives Firmware-Image

Jeweils eines der beiden Firmware-Images ist aktiv (running), während das andere inaktiv ist. Welches Firmware-Image aktiv ist, wird über den so genannten Firmware-Selektor festgelegt (siehe Seite 368).

Struktur des iRMC S2/S3-EEPROM

Der EEPROM des iRMC S2/S3 enthält je einen Bereich für Firmware-Image 1 und Firmware-Image 1:

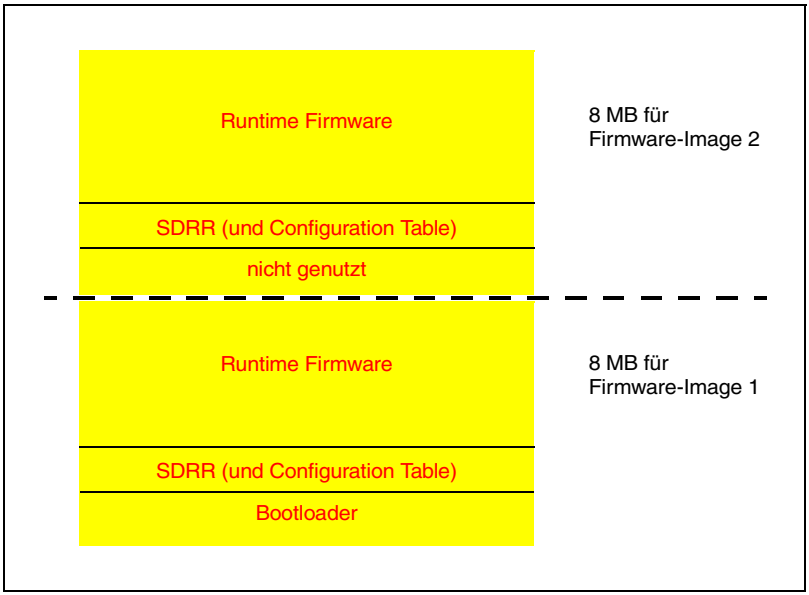


Bild 217: Struktur des iRMC S2/S3-EEPROM

– Bootloader

  Der Bootloader prüft das zurzeit aktive Firmware-Image. Bei fehlerhafter Firmware setzt der Bootloader den Firmware-Selektor auf das andere Firmware-Image.

– SDRR (Sensor Data Record Repository)

  Das SDRR enthält die Sensor Data Records (SDR), in denen Sensor-Informationen des verwalteten Servers abgelegt sind. Außerdem dient das SDRR als Schnittstelle, über die Sie auf die SDRs zugreifen können.

– Runtime Firmware

  Die Runtime Firmware stellt den ablauffähigen Teil der Firmware des iRMC S2/S3 dar.

Für jeden dieser Bereiche können Sie eine Firmware-Aktualisierung durchführen.

Firmware-Selektor

Der Firmware-Selektor spezifiziert die Firmware des iRMC S2/S3, die ausgeführt wird. Nach jedem Reset und Neustart des iRMC S2/S3 wird der Firmware-Selektor ausgewertet und es wird auf die entsprechende Firmware verzweigt.

Der Firmware-Selektor kann folgende Werte annehmen:

0 Firmware-Image mit der neuesten Firmware-Version

1 Firmware-Image 1

2 Firmware-Image 2

3 Firmware-Image mit dem ältesten Firmware-Version

4 Firmware-Image, das zuletzt aktualisiert wurde

5 Firmware-Image, das am längsten nicht mehr aktualisiert wurde

Je nach verwendeter Update-Variante ist der Firmware-Selektor nach erfolgtem Update unterschiedlich gesetzt.

Den Firmware-Selektor können Sie abfragen und explizit setzen

– auf der Seite *iRMC S2/S3 Information* der iRMC S2/S3-Web-Oberfläche (siehe "Aktive Firmware" auf Seite 173)

oder

– mithilfe des Flash-Tools (siehe Seite 381)

10.2 USB Memory Stick erstellen

Den USB Memory Stick benötigen Sie **nicht**, wenn Sie die Firmware des iRMC S2/S3 auf einem der folgenden Wege aktualisieren:

- mithilfe des ServerView Update Managers
- mithilfe des ServerView Update Manager Express oder via ASP
- via iRMC S2/S3-Web-Oberfläche und TFTP-Server

Gehen Sie wie folgt vor:

- Laden Sie die Firmware *Firmware Update for USB Stick* aus der Download-Section des Web-Servers von Fujitsu Technology Solutions in ein Verzeichnis auf Ihrem Rechner.

  In Ihrem Download-Verzeichnis finden Sie das ZIP-Archiv *FTS_<spec>.zip*. (Der Namensbestandteil *<spec>* enthält Informationen zu Systemtyp, Systembaugruppe, Firmware/SDRR-Version etc.):

  Das Zip-Archiv enthält folgende Dateien:

  - *USBImage.exe*
  - *iRMC_<Firmware-Version>.exe*
  - *iRMC_<Firmware-Version>.IMA*

- Verbinden Sie den USB Memory Stick mit Ihrem Rechner.
- Starten Sie die Datei *iRMC_<Firmware-Version>.exe* oder die Datei *USBImag.exe*.

  Je nachdem, welche Datei Sie aufrufen, wird eines der folgenden Fenster geöffnet (siehe Bild 218 auf Seite 370):

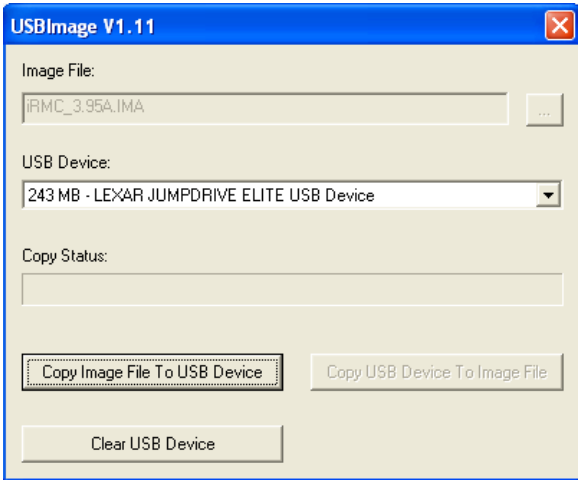


Bild 218: Image-Datei auf USB Memory Stick kopieren (iRMC_<Firmware-Version>.exe)

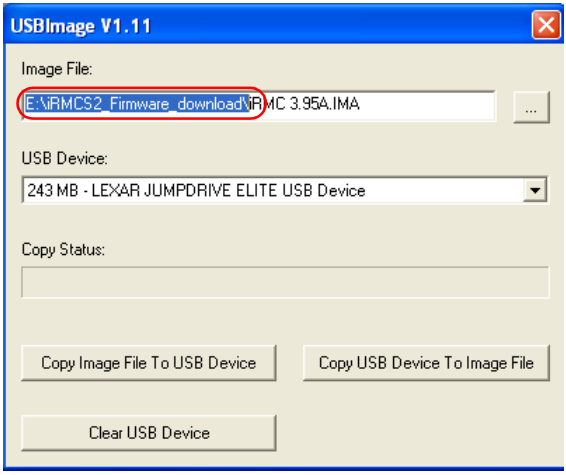


Bild 219: Image-Datei auf USB Memory Stick kopieren (USBImage.exe)

Wenn Sie *USBImag.exe* aufgerufen haben, müssen Sie unter *Image File:* die Datei *iRMC_<Firmware-Version>.IMA* explizit angeben.

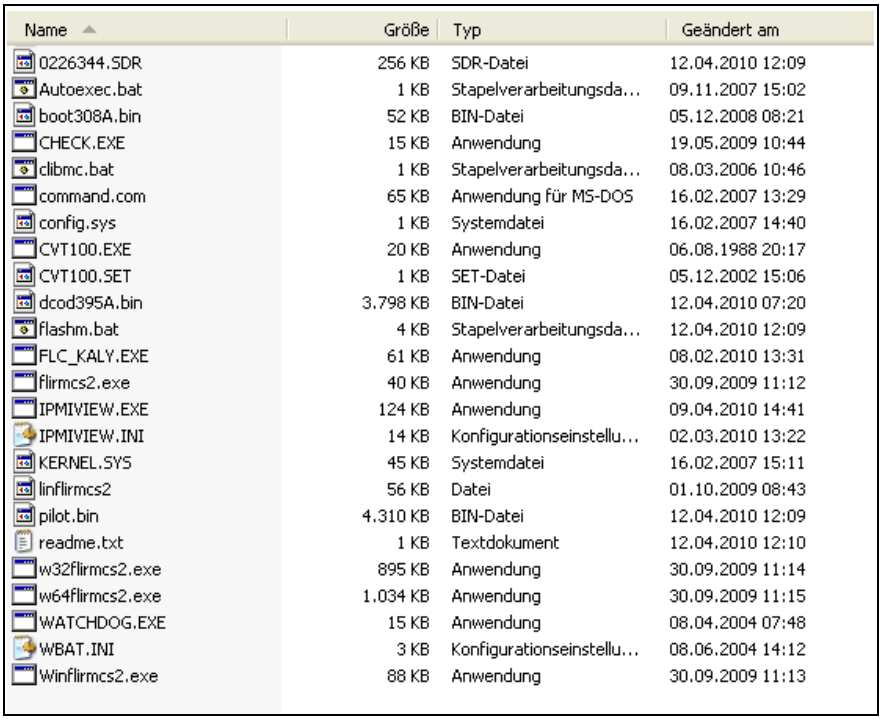
► Klicken Sie auf *Clear USB Device*, um die Daten auf dem USB Memory Stick zu löschen.

► Klicken Sie auf *Copy Image File to USB Device*, um die Datei *BMC_<Firmware-Version>.IMA* auf den USB Memory Stick zu kopieren und zu extrahieren.

ACHTUNG!

Durch diese Aktion wird der Inhalt des USB Memory Sticks überschrieben!

Nach Abschluss des Kopiervorgangs befinden sich Flash-Tools und Image-Dateien auf dem USB Memory Stick:



Name	Größe	Typ	Geändert am
0226344.SDR	256 KB	SDR-Datei	12.04.2010 12:09
Autoexec.bat	1 KB	Stapelverarbeitungsda...	09.11.2007 15:02
boot308A.bin	52 KB	BIN-Datei	05.12.2008 08:21
CHECK.EXE	15 KB	Anwendung	19.05.2009 10:44
clibmc.bat	1 KB	Stapelverarbeitungsda...	08.03.2006 10:46
command.com	65 KB	Anwendung für MS-DOS	16.02.2007 13:29
config.sys	1 KB	Systemdatei	16.02.2007 14:40
CVT100.EXE	20 KB	Anwendung	06.08.1988 20:17
CVT100.SET	1 KB	SET-Datei	05.12.2002 15:06
dcod395A.bin	3.798 KB	BIN-Datei	12.04.2010 07:20
flashm.bat	4 KB	Stapelverarbeitungsda...	12.04.2010 12:09
FLC_KALY.EXE	61 KB	Anwendung	08.02.2010 13:31
flirmcs2.exe	40 KB	Anwendung	30.09.2009 11:12
IPMIVIEW.EXE	124 KB	Anwendung	09.04.2010 14:41
IPMIVIEW.INI	14 KB	Konfigurationseinstellu...	02.03.2010 13:22
KERNEL.SYS	45 KB	Systemdatei	16.02.2007 15:11
linflirmcs2	56 KB	Datei	01.10.2009 08:43
pilot.bin	4.310 KB	BIN-Datei	12.04.2010 12:09
readme.txt	1 KB	Textdokument	12.04.2010 12:10
w32flirmcs2.exe	895 KB	Anwendung	30.09.2009 11:14
w64flirmcs2.exe	1.034 KB	Anwendung	30.09.2009 11:15
WATCHDOG.EXE	15 KB	Anwendung	08.04.2004 07:48
WBAT.INI	3 KB	Konfigurationseinstellu...	08.06.2004 14:12
Winflirmcs2.exe	88 KB	Anwendung	30.09.2009 11:13

Bild 220: Image-Dateien und Flash-Tools auf dem USB Memory Stick.

10.3 Firmware-Image aktualisieren

Da die Firmware des iRMC S2/S3 im SRAM-Speicher des iRMC S2/S3 ausgeführt wird, können Sie sowohl das aktive als auch das inaktive Firmware-Image online, d.h. bei laufendem Server-Betriebssystem aktualisieren.

Für den Update der Firmware-Images stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Update über die iRMC S2/S3 Web-Oberfläche

– Update mithilfe des ServerView Update Managers

– Update mithilfe des ServerView Update Manager Express oder via ASP

– Update mithilfe der Betriebssystem-Flash-Tools.

Firmware auf den Vorgängerstand zurücksetzen (Firmware Downgrade)

Neben der Firmware-Aktualisierung besteht auch die Möglichkeit zum Firmware-Downgrade, d.h. Sie können die Firmware auf den Stand der Vorgängerversion zurücksetzen.

Als einfachste Möglichkeit für einen Downgrade bietet es sich an, das Firmware-Image der Vorgängerversion als inaktives Firmware-Image im EEPROM des iRMC S2/S3 in Reserve zu halten. Bei Bedarf setzen Sie den Firmware-Selektor auf das Firmware-Image der Vorgängerversion (siehe Seite 188) und starten anschließemd den iRMC S2/S3 neu, um die Firmware zu aktivieren.

Darüber hinaus können Sie für den Firmware-Downgrade auch die in den folgenden Abschnitten vorgestellten Verfahren einsetzen, indem Sie den Update mit der Firmware der Vorgängerversion durchführen. Falls für den Downgrade Besonderheiten zu beachten sind, wird im Folgenden an den entsprechenden Stellen gesondert darauf hingewiesen.

10.3.1 Update über die iRMC S2/S3-Web-Oberfläche

Über die Seite *iRMC S2/S3 Firmware Aktualisierung* können Sie die Firmware des iRMC S2/S3 aktualisieren, indem Sie das gewünschte Firmware Image wahlweise lokal am Remote-Arbeitsplatz oder auf einem TFTP-Server zur Verfügung stellen (siehe Abschnitt "iRMC S2/S3 Firmware Aktualisierung" auf Seite 187).

10.3.2 Update via ServerView Update Manager

Mithilfe des ServerView Update Managers können Sie den Update der iRMC S2/S3-Firmware über eine grafische Benutzeroberfläche (Windows) oder über ein Command Line Interface (Windows und Linux) starten. Der ServerView Update Manager greift auf die Update-Daten über sein Update-Repository auf der ServerView Suite DVD 1 oder dem Management-Server zu. Das Update-Repository auf dem Management-Server aktualisieren Sie mittels Download-Manager oder manuellem Download aus der Download Section des Web-Servers von Fujitsu Technology Solutions.

Näheres zum Firmware-Update mit dem ServerView Update Manager finden Sie im Handbuch „ ServerView Update Manager“.

10.3.3 Online-Update via ServerView Update Manager Express oder ASP

Unter Windows- und Linux-Betriebssystemen können Sie die iRMC S2/S3-Firmware wahlweise mithilfe der grafischen Benutzeroberfläche des ServerView Update Manager Express aktualisieren oder Sie verwenden die ASPs (Autonomous Support Package)-Kommandoschnittstelle.

Unter Windows können Sie ein ASP außerdem im Windows-Explorer per Doppelklick auf die entsprechende ASP-**.exe*-Datei starten.

Beachten Sie beim Firmware-Downgrade:

– Bei Downgrade via Update Manager Express:

  Der Firmware-Downgrade ist nur im *Expert*-Mode bei gleichzeitig aktivierter *Downgrade*-Option möglich.

– Bei Downgrade via ASP:

  – Unter Windows:

    Downgrade ist möglich, wenn Sie das ASP per Doppelklick auf die entsprechende ASP-**.exe*-Datei starten. Falls sie das ASP über die Kommandoschnittstelle (CLI) starten, müssen Sie die Option *Force=yes* explizit angeben.

  – Unter Linux:

    Sie müssen die Option *-f* bzw. *--force* explizit angeben.

Näheres zum Firmware-Update via Update Manager Express und ASP finden Sie im Handbuch „Lokaler System-Update von PRIMERGY Servern“.

10.3.4 Update mit den Betriebssystem-Flash-Tools

Ein Update mithilfe der Betriebssystem-Flash-Tools wird nur als Recovery Flash durchgeführt, d.h. es erfolgt keine Versionsprüfung.

Voraussetzung:

Die Flash-Tools sowie die Dateien für den Fimware-Update müssen im Dateisystem des verwalteten Servers vorhanden sein.

Abhängig vom eingesetzten Betriebssystem verwenden Sie eines der folgenden Flash-Tools:

DOS:	flirmcs2
Windows:	winflirmcs2 **Voraussetzung:** Auf dem verwalteten Server müssen die ServerView-Agenten für die verwendete Windows-Variante (32/64 bit) gestartet sein.
Windows (32 bit):	win32flirmcs2 (Agenten sind nicht erforderlich.)
Windows (64 bit):	win64flirmcs2 (Agenten sind nicht erforderlich.)
Linux:	linflirmcs2

Die Flash-Tools rufen Sie in der Windows-Eingabeaufforderung (flirmcs2, winflirmcs2, win32flirmcs2, win64flirmcs2) bzw. am Linux-CLI (linflirmcs2) auf.

Syntax und Operanden der Flash-Tools sind beschrieben im Abschnitt "Flash-Tools" auf Seite 381.

Gehen Sie wie folgt vor:

Nachfolgend ist der Online-Update unter Verwendung eines USB Memory Sticks beschrieben (siehe Abschnitt "USB Memory Stick erstellen" auf Seite 369).

- Verbinden Sie den USB Memory Stick mit dem verwalteten Server.
- Wechseln Sie in der Windows-Eingabeaufforderung oder im Command Line Interface (CLI) von Linux zum Laufwerk des USB Memory Sticks.
- Setzen Sie den Firmware-Selektor auf den Wert 4, indem Sie das Flash-Tool mit dem Parameter */s 4* aufrufen.

  Z.B. geben Sie in der Windows-Eingabeaufforderung an:

  ```
  WinFLIRMCS2 /s 4
  ```

- Starten Sie den Update der Firmware und der SDR-Daten, indem Sie das Flash-Tool mit den entsprechenden Update-Dateien aufrufen.

  Z.B. geben Sie in der Windows-Eingabeaufforderung an:

  ```
  WinFLIRMCS2 dcod<firmware-version>.bin <nnnnnnn>.sdr /i
  ```

  Während des Firmware-Updates werden Sie an der Konsole über den Verlauf des Update-Vorgangs informiert. Im Fehlerfall wird der Update-Vorgang abgebrochen und ein entsprechender Returncode gemeldet (siehe Seite 383).

- Starten Sie den verwalteten Server neu. Das Firmware-Image mit der aktualisierten Firmware wird dadurch automatisch aktiviert.

10.3.5 Update über das Menü der FlashDisk

Für den Update über das Menü der FlashDisk benötigen Sie einen bootfähigen USB Memory Stick (siehe Abschnitt "USB Memory Stick erstellen" auf Seite 369).

Gehen Sie wie folgt vor:

- Verbinden Sie den USB Memory Stick mit dem verwalteten Server (direkt oder via Remote Storage).
- Booten Sie vom USB Memory Stick.

Nach Abschluss des Bootvorgangs werden die Daten des USB Memory Sticks automatisch in eine RAM Disk kopiert. Anschließend wird die Datei *autoexec.bat* automatisch gestartet.

Das FlashDisk-Menü wird geöffnet:

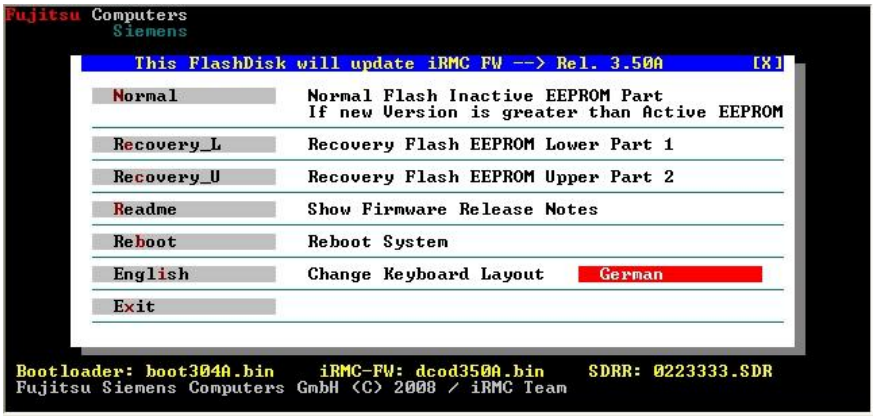


Bild 221: Menü der FlashDisk

Ein Firmware-Downgrade ist nur via Recovery Flash möglich.

Normal

Es wird ein *Normal Flash* durchgeführt.

Bei einem Normal Flash werden die Bereiche des EEPROM auf Aktualität überprüft, die die aktive Firmware enthalten. Ist einer dieser Bereiche nicht aktuell, so wird der korrespondierende Bereich für die inaktive Firmware aktualisiert, sofern dieser Bereich nicht bereits aktuell ist.

Recovery _L

Es wird ein *Recovery Flash* für das Firmware-Image 1 (untere Firmware-Image) durchgeführt.

Bei einem Recovery Flash wird der Flash ohne Versionsprüfung für alle drei Bereiche des Firmware-Image 1 durchgeführt.

Recovery _U

Es wird ein *Recovery Flash* für das Firmware-Image 2 (oberes Firmware-Image) durchgeführt.

Bei einem Recovery Flash wird der Flash ohne Versionsprüfung für alle drei Bereiche des Firmware-Image 2 durchgeführt.

Readme

Die Readme-Datei mit wird angezeigt.

Reboot

Es wird ein Warmstart des iRMC S2/S3 durchgeführt.

English / *German*

Tastatur-Layout festlegen. Standardmäßig ist *German* eingestellt.

- Starten Sie die gewünschte Update-Variante durch Anklicken der entsprechenden Schaltfläche.

  Während des Firmware-Updates werden Sie an der Konsole über den Verlauf des Update-Vorgangs informiert. Im Fehlerfall wird der Update-Vorgang abgebrochen. Ein entsprechender Returncode wird gemeldet (siehe Seite 383).

- Klicken Sie nach Abschluss des Update-Vorgangs auf *Exit*, um das FlashDisk-Menü zu verlassen.

- Trennen Sie den USB Memory Stick vom verwalteten Server.

- Starten Sie den verwalteten Server neu (z.B. mit Ctrl + Alt + Entf).

10.4 Emergency Flash

Wenn die Firmware des iRMC S2/S3 nicht mehr ausgeführt werden kann, z. B. weil die SDRs nicht mit dem System kompatibel sind, können Sie über den Emergency Mode die Firmware wieder zum Laufen bringen. Im Emergency Mode verzweigt das System automatisch zum Bootloader und ist dann bereit für den Firmware-Update.

Der Emergency Mode wird durch abwechselndes Blinken von Fehler-LED (Global Error LED) (rot) und Identifizierungs-LED (blau) angezeigt.

Um den verwalteten Server in den Emergency Mode zu versetzen und anschließend die Firmware des iRMC S2/S3 zu aktualisieren, verfahren Sie wie folgt:

- Ziehen Sie den Netzstecker.
- Stecken Sie den Stecker bei gedrückter Identify-Taste wieder in die Steckdose.

  Der verwaltete Server befindet sich nun im Emergency Mode.
- Booten Sie den Server nach DOS und aktualisieren Sie die Firmware des iRMC S2/S3 per Recovery Flash.

  Wenn die Firmware nicht aktiv ist, startet der Bootvorgang mit einer zeitlichen Verzögerung von bis zu 2 Minuten. Die Fehlermeldung „iRMC S2/S3 Controller Error“, die das BIOS während dieser Zeit ausgibt, können Sie ignorieren.

10.5 Flash-Tools

Die Tools WinFLIRMCS2, rFLIRMCS2 und sFLIRMCS2 unterscheiden sich von flirmcs2 nur im Tool-Namen sowie in der Umgebung, in der sie aufgerufen werden. Die nachfolgende Beschreibung gilt somit auch für die Tools WinFLIRMCS2, rFLIRMCS2 und sFLIRMCS2. Anstelle von „flirmcs2“ ist dabei jeweils „WinFLRMCS2“, „rFLIRMCS2“ bzw. sFLIRMCS2 anzugeben.

Syntax

```
flirmcs2 {/v|/o [/4]|/s[<Wert>]}

flirmcs2 {<datei1> [<datei2>] [<datei3>]
      [/n /l[<logdatei>] /d /e /4 /i]}

flirmcs2 {/h|/?}
```

Optionen

/v Aktuellen Versionsstand des Kommandos anzeigen.

/o Aktuelle Versionsstände beider Firmware-Images anzeigen.

/s Aktuellen Wert des Firmware-Selektors anzeigen.

/s <Wert>
Wert des Firmware-Selektors setzen. Mit dieser Option spezifizieren Sie das Firmware-Image, dessen Firmware nach einem Firmware-Reset gestartet wird.

- 0 Selektor auf das Firmware-Image mit der neuesten Firmware setzen.
- 1 Selektor auf den Firmware-Image 1 setzen.
- 2 Selektor auf den Firmware-Image 2 setzen.
- 3 Selektor auf das Firmware-Image mit der ältesten Firmware setzen.
- 4 Selektor auf das Firmware-Image mit der zuletzt aktualisierten Firmware setzen.
- 5 Selektor auf das Firmware-Image mit der am längsten nicht mehr aktualisierten Firmware setzen.

<datei1> bis <datei3>

Mit der Angabe einer oder mehrerer Dateien legen Sie fest, welche Aktualisierung(en) vorgenommen werden soll(en). Folgende Dateien stehen zur Auswahl:

boot<FW-Version>.bin

Aktualisierung der Bootloader-Firmware.

dcod<FW-Version>.bin

Aktualisierung der Runtime-Firmware.

<SDR-Version>.SDR

Aktualisierung des SDR-Datensatzes.

Für eine Aktualisierung des Firmware-Image 2 müssen Sie auch die Option */4* angeben (siehe unten).

/4 Firmware-Image 2 aktualisieren.

/l [<logdatei>]

Ausgabe von Fehlermeldungen in die angegebene Logdatei. Wenn Sie Logdatei angeben, erfolgt die Ausgabe in die Datei *flbmc.log*.

/n Keine Ausgabe auf der Konsole.
Diese Option übersteuert die Optionen */p* und */d*.

/np Anstelle der Prozent-Anzeige wird während des Flashens ein drehender Strich ausgegeben.

/d Ausgabe zusätzlicher Debug-Informationen.

/e Emulationsmodus (nur für Debug-Zwecke).

/i Inaktives Firmware-Image aktualisieren.

/h und /?

Ausgabe von Hilfe-Informationen.

Rückgabewerte

0	Aktualisierung erfolgreich ausgeführt.
1	Unzulässige oder fehlende Optionen.
3	PROM-Typ nicht verfügbar.
4	Kommunikation mit iRMC S2/S3 nicht möglich.
5	Fehlerhaft Binärdatei.
8	Fehler beim Zugriff auf die Keyboard Control Style-Schnittstelle (KCS).
9	Zeitüberschreitung während der Kommunikation mit dem Ziel-EEPROM.
10	Kein Pufferspeicher zugewiesen.
12	Netzknoten belegt.
13	Zeitüberschreitung beim Löschen des EEPROM.
14	Zeitüberschreitung bei der Aktualisierung des EEPROM.
15	Fehler beim Löschen des EEPROM.
16	Fehler bei der Aktualisierung des EEPROM.

11 Remote-Installation des Betriebssystems via iRMC S2/S3

Dieses Kapitel beschreibt, wie Sie mithilfe des ServerView Installation Managers (im Folgenden kurz Installation Manager) sowie mittels der iRMC S2/S3-Features „Advanced Video Redirection (AVR)“ und „Remote Storage vom Remote-Arbeitsplatz aus das Betriebssystem auf dem verwalteten Server installieren.

Im Einzelnen informiert das Kapitel über folgende Themen:

– Generelles Vorgehen bei der Remote-Installation eines Betriebssystems mithilfe von Remote Storage-Speichermedien.

– Verwalteten Server vom Remote-Arbeitsplatz aus über die ServerView DVD 1 booten (Windows und Linux).

– Windows nach Konfiguration auf dem verwalteten Server vom Remote-Arbeitsplatz aus installieren.

– Linux nach Konfiguration auf dem verwalteten Server vom Remote-Arbeitsplatz aus installieren.

Die Beschreibung legt den Schwerpunkt auf das Handling der Remote Storage-Speichermedien. Kenntnisse der Funktionalität des Installation Managers werden vorausgesetzt (siehe Handbuch „ServerView Installation Manager“).

Voraussetzungen für eine Remote-Installation des Betriebssystems via iRMC S2/S3:

– Die LAN-Schnittstelle des iRMC S2/S3 muss konfiguriert sein (siehe Seite 43).

– Der Lizenzschlüssel (License Key) für die Nutzung der iRMC S2/S3-Funktionen „Grafische Konsolen-Umleitung“ und „Remote Storage“ muss installiert sein (siehe Seite 174).

11.1 Betriebssystem via iRMC S2/S3 installieren - generelles Vorgehen

Die Remote-Installation des Betriebssystems via iRMC S2/S3 ist aus Sicht des Installation Managers eine lokale Konfiguration und Installation des Betriebssystems auf dem verwalteten Server, die Sie vom Remote-Arbeitsplatz aus über das AVR-Fenster mithilfe von Remote Storage-Speichermedien durchführen.

Im Einzelnen sind für eine Installation mittels Installation Manager folgende Schritte erforderlich:

1. Speichermedium (DVD 1 oder Installation Manager Boot-Image), von dem gebootet werden soll, als Remote Storage verbinden.
2. Verwalteten Server vom Remote-Arbeitsplatz aus über die DVD 1 oder Installation Manager Boot-Image booten und konfigurieren.
3. Betriebssystem via Installation Manager vom Remote-Arbeitsplatz aus auf dem verwalteten Server installieren.
4. Mauszeiger-Synchronisation im AVR-Fenster optimieren (nur unter Linux erforderlich).

Windows ohne Installation Manager mithilfe der Windows-Installations-CD/DVDs installieren

Die Remote-Installation von Windows via Remote Storage können Sie wahlweise mithilfe des Installation Managers oder ausschließlich mithilfe der Windows-Installations-CD/DVDs durchführen. Hinsichtlich des Handlings der Remote Storage-Speichermedien stimmen beide Verfahren überein.

Aus folgenden Gründen empfiehlt sich jedoch eine Windows-Installation mithilfe des Installation Managers:

– Der Installation Manager ermittelt selbstständig die erforderlichen Treiber und kopiert diese in das System.

– Während der Installation stehen Ihnen alle Installation Manager-Funktionen zur Verfügung. So können Sie z.B. das gesamte System inklusive der Einstellungen für das Server-Management konfigurieren.

– Die Installation ohne Installation Manager müssen Sie über die Tastatur steuern, da während des Installationsvorgangs der Mauszeiger nicht synchronisiert werden kann. Dagegen können Sie bei der Installation via Installation Manager die gesamte Konfiguration und Installation mithilfe der Maus abwickeln.

– Bei der Installation ohne Installation Manager müssen Sie alle erforderlichen Einstellungen für die Synchronisation des Mauszeigers nachträglich „von Hand“ durchführen.

– Die Installation via Installation Manager dauert nicht wesentlich länger als die Installation mithilfe der Betriebssystem-CD/DVDs.

Linux ohne Installation Manager mithilfe der Linux-Installations-CD/DVD installieren

Wenn Sie die vom System benötigten Treiber kennen, können Sie die Linux-Installation auch durch Booten von der Linux-Installations CD/DVD starten.

Falls die Installation eine Treiber-Integration von der Floppy-Disk erfordert, müssen Sie vor Beginn der Installation jeweils eine Remote Storage-Verbindung einrichten

– zum Speichermedium (CD-ROM/DVD-ROM oder ISO Image), von dem aus gebootet werden soll, sowie

– ggf. Speichermedium für die Treiber-Installation.

11.2 Speichermedium als Remote Storage verbinden

Remote Storage stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich an anderer Stelle im Netz befindet.

Die Source für das virtuelle Laufwerk kann sein:

– Physisches Laufwerk oder Image-File am Remote-Arbeitsplatz. Das Image-File kann außerdem auf einem Netzlaufwerk liegen (mit Laufwerksbuchstaben, z. B. „D:“ für Laufwerk D).

– Image-File, das mithilfe eines Remote Storage Servers zentral im Netz bereitgestellt wird.

Parallele Remote Storage-Verbindungen:

Zur selben Zeit möglich sind entweder

– **maximal zwei** Remote Storage-Verbindungen zu virtuellen Laufwerken am Remote-Arbeitsplatz (bei Verbindungsaufbau via AVR Java-Applet)

oder

– **eine** Remote Storage-Verbindung zu einem Remote Storage Server.

Remote Storage-Verbindungen via Applet und Remote Storage Server sind nicht gleichzeitig möglich.

Mithilfe der Seite *Remote Storage* der iRMC S2/S3-Web-Oberfläche können Sie sich über den Status der aktuellen Remote Storage-Verbindungen informieren (siehe Seite 323).

Ausführliche Informationen zu Remote Storage finden Sie im Kapitel "Remote Storage" auf Seite 117.

Speichermedium am Remote-Arbeitsplatz als Remote Storage verbinden

Zum Herstellen der Remote Storage-Verbindung gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Melden Sie sich mit Remote Storage Enabled-Berechtigung an der iRMC S2/S3-Web-Oberfläche an (siehe Seite 142).
- Öffnen Sie die Seite *Grafische Konsolen-Umleitung (AVR)* und starten Sie die AVR (siehe Seite 312).

- Starten Sie im AVR-Fenster „Remote Storage“ (siehe Seite 120).
- Stellen Sie die Speichermedien für Remote Storage bereit (siehe Seite 123):
  - Bei Installation via Installation Manager:

    ServerView Suite DVD 1 oder Installation Manager Boot-Image sowie optional einen formatierten USB Memory Stick als Status-Backup-Medium
  - Bei Installation via Installations-CD/DVD des Herstellers: Windows oder Linux Installations-CD/DVD und optionale Treiber.

    Es wird empfohlen, die ServerView Suite DVD 1 bzw. die Betriebssystem-Installations-CD/DVD als Image-Datei (ISO Image) in einem Verzeichnis abzulegen und von dort als Remote Storage zu verbinden oder via Remote Storage Server zur Verfügung zu stellen.

  Die bereitgestellten Speichermedien werden in der Dialogbox *Storage Devices* angezeigt:

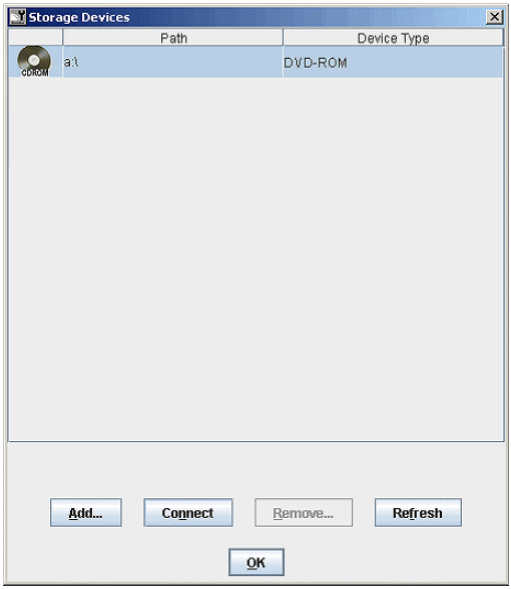


Bild 222: Dialogbox Storage Devices: ServerView Suite DVD 1

- Klicken Sie auf *Connect*, um das DVD-ROM-Laufwerk (DVD 1) oder das Installation Manager Boot-Image als Remote Storage zu verbinden.

Vom Remote Storage Server bereitgestelltes ISO Image (Image-File) als Remote Storage verbinden

Ein via Remote Storage Server bereitgestelltes Image-File können Sie zum Booten von einem Installation Manager Boot-Image verwenden.

Die Nutzung eines via Remote Storage Server bereitgestellten virtuellen Laufwerks setzt voraus, dass der Remote Storage Server installiert und gestartet ist (siehe Abschnitt "Remote Storage via Remote Storage Server bereitstellen" auf Seite 133).

Zum Erstellen der Verbindung zu Remote Storage Server gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Melden Sie sich mit *Remote Storage Enabled*-Berechtigung an der iRMC S2/S3-Web-Oberfläche an (siehe Seite 142).
- Wählen Sie die Seite *Remote Storage*.
- Stellen Sie die Verbindung zum Remote Storage Server her (siehe Seite 325).

11.3 Verwalteten Server von der ServerView Suite DVD 1 booten und via Installation Manager konfigurieren

Gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Schalten Sie über die iRMC S2/S3-Web-Oberfläche den verwalteten Server ein oder starten Sie den Server neu (siehe Seite 196). Den Bootvorgang können Sie im AVR-Fenster verfolgen.

  Während der BIOS/TrustedCore/UEFI POST-Phase des verwalteten Servers werden Remote Storage-Speichermedien als USB 2.0 Geräte angezeigt. Remote Storage-Speichermedien werden durch die folgenden Einträge in der Boot-Sequenz des BIOS repräsentiert:

  – Eine (physische) Floppy-Disk wird durch einen eigenen Eintrag „FTS RemoteStorage FD-(USB 2.0)“ repräsentiert.

  – Alle anderen Remote Storage Geräte-Typen werden durch einen gemeinsamen Eintrag „CD-ROM DRIVE“ repräsentiert.

  > **i** Wenn am verwalteten Server gleichzeitig ein lokales CD-ROM/DVD-ROM-Laufwerk und ein als Remote Storage verbundenes CD-ROM/DVD-ROM-Laufwerk angeschlossen sind, bootet der verwaltete Server vom Remote Storage CD-ROM/DVD-ROM-Laufwerk.

- Drücken Sie während des Boot des Servers die Taste F2.
- Rufen Sie im BIOS/TrustedCore/UEFI-Setup das Menü *Boot* für die Festlegung der Boot-Sequenz auf.
- Spezifizieren Sie die Boot-Priorität 1 (höchste Priorität) für die als Remote Storage verbundene DVD 1.
- Sichern Sie Ihre Einstellungen und verlassen Sie das BIOS/TrustedCore/UEFI-Setup.

Danach bootet der verwaltete Server von der als Remote Storage verbundenen ServerView Suite DVD 1.

Falls das System nicht vom Remote Storage-Speichermedium (ServerView Suite DVD 1 oder Installation Manager Boot-Image) bootet:

- ► Prüfen Sie, ob das Speichermedium während der BIOS POST-Phase angezeigt wird, und verbinden Sie erforderlichenfalls das Speichermedium als Remote Storage.
- ► Stellen Sie die korrekte Boot-Reihenfolge sicher.

Das Booten von der ServerView Suite DVD 1 via Remote Storage-Speichermedium dauert ca. 5 Minuten. Während des Bootens werden Sie über den Fortschritt des Bootvorgangs informiert.

Nach Abschluss des Bootvorgangs fordert Sie eine Dialogbox auf, ein Medium für den Statussicherungsbereich (Status-Backup-Medium) auszuwählen.

Bevor Sie mit der Installation des Betriebssystems beginnen, sollten Sie im AVR-Fenster am Remote-Arbeitsplatz den lokalen Mauszeiger und den Mauszeiger des verwalteten Servers synchronisieren. Näheres zur Synchronisation der Mauszeiger im AVR-Fenster finden Sie im Abschnitt "Mauszeiger synchronisieren" auf Seite 100.

► Wählen Sie unter *Installation Manager Modus* den *Standard Modus*.

► Legen Sie fest, ob die Konfigurationsdaten auf einem lokalen Wechseldatenträger oder einem Netzwerkmedium gespeichert werden sollen:

Beachten Sie: Wenn Sie keine Option zur Statussicherung wählen, gehen sämtliche Konfigurationsdaten bei einem Reboot verloren.

Medium zur Statussicherung

Das Backup-Medium darf nicht schreibgeschützt sein.

Ein USB-Stick muss bereits beim Systemstart am USB-Port angeschlossen sein. Falls dies versäumt wurde und Sie die Konfigurationsdatei abspeichern wollen:

Schließen Sie den USB-Stick jetzt an und starten Sie einen Reboot von der ServerView Suite DVD 1.

► Wählen Sie die Option *auf lokalem Laufwerk (Diskette / USB Stick)*.

► Wählen Sie im Auswahlfeld rechts von der Option das entsprechende Laufwerk aus.

Nähere Informationen zur Erzeugung von Installation Manager-Statusdisketten erhalten Sie im Handbuch „ServerView Installation Manager“.

Statusmedium und/oder Installationsmedien über das Netzwerk anbinden

► Treffen Sie zu diesem Zweck die erforderlichen Freigaben.

Wenn Sie ein Medium mit einer vorbereiteten Konfigurationsdatei und/oder ein Installationsmedium via Netz bereitstellen, müssen Sie diese Option wählen. Für die aktuelle Installation Manager-Sitzung können Sie, abhängig von Ihrer Infrastruktur, entweder eine temporäre IP-Adresse via DHCP beziehen oder manuell eine IPv4- oder IPv6-Adresse konfigurieren.

► Starten Sie den Installation Manager durch Klicken auf *Weiter*.

Lokales Deployment starten

Nach dem Start des Installation Managers wird das Begrüßungsfenster angezeigt:

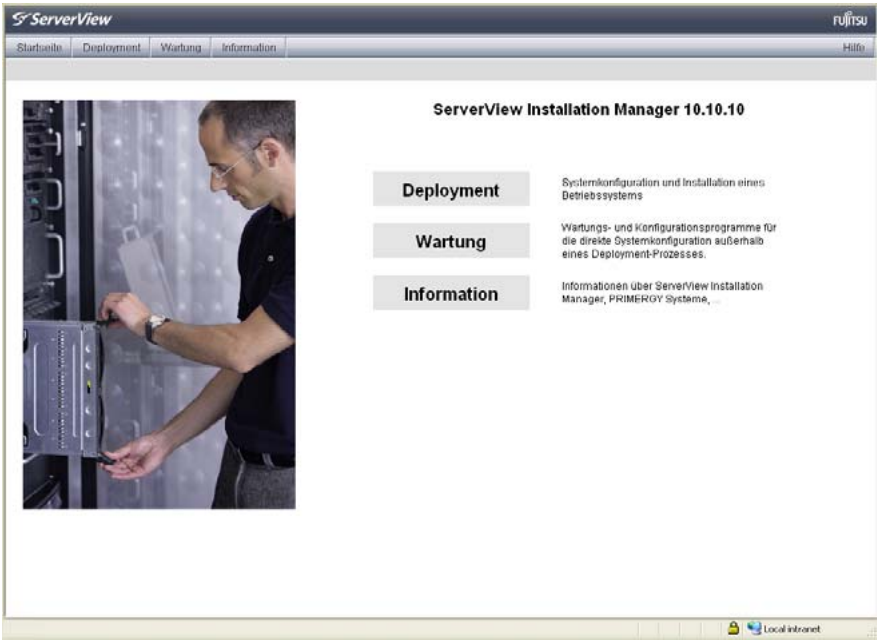


Bild 223: Installation Manager - Begrüßungsfenster

► Klicken Sie auf *Deployment*, um die Vorbereitung der lokalen Installation (Deployment) zu starten.

Zur Vorbereitung der Installation werden Sie von den Wizards des Installation Managers durch eine Folge von Konfigurationsschritte geführt, in denen Sie die Vorgaben für die Konfiguration des Systems sowie für die anschließende bedienerlose Betriebssystem-Installation zusammenzustellen.

Konfigurieren Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers. Dann können Sie die Windows Installations-CD/DVD auch über das CD-ROM/DVD-ROM-Laufwerk des Remote-Arbeitsplatzes

bereitstellen, wenn Sie dieses als Remote Storage mit dem verwalteten Server verbinden (siehe Abschnitt "Windows nach Konfiguration auf dem verwalteten Server installieren" auf Seite 396).

Nach Abschluss der Konfiguration mit dem Installation Manager wird der Dialog *Installationsparameter* für die Windows-Installation (siehe Seite 396) bzw. für die Linux-Installation (siehe Seite 399) angezeigt, über den Sie den installationsprozess starten können.

11.4 Betriebssystem nach Konfiguration auf dem verwalteten Server installieren

Im Anschluss an die Konfiguration installieren Sie das Betriebssystem auf dem verwalteten Server.

11.4.1 Windows nach Konfiguration auf dem verwalteten Server installieren

Nach Abschluss der Konfiguration zeigt der Installation Manager folgenden Dialog an:

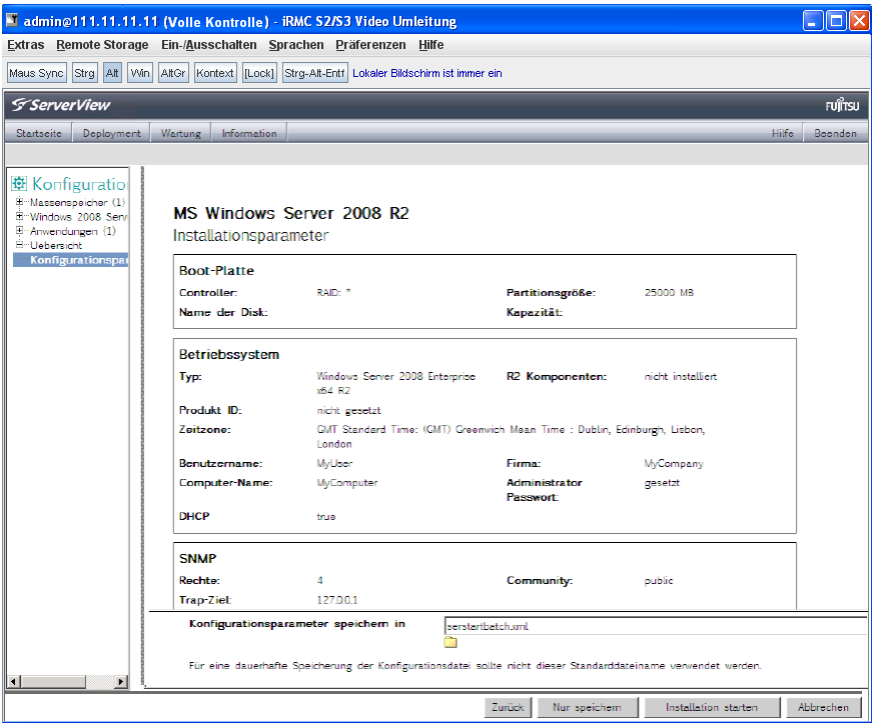


Bild 224: Installation Manager - Installation starten

Wenn Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers konfiguriert haben, gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Trennen Sie Ihre zurzeit aktiven Remote Storage-Verbindungen. Näheres zum Trennen von Remote Storage-Verbindungen finden Sie auf Seite 131.
- Entfernen Sie die ServerView Suite DVD 1 aus dem DVD-ROM-Laufwerk am Remote-Arbeitsplatz.
- Legen Sie die Windows-Installations-CD/DVD in dieses DVD-ROM-Laufwerk ein.

  Schließen Sie die Anwendung, falls *autostart* aktiviert ist.

- Verbinden Sie das CD-ROM/DVD-ROM-Laufwerk, das die Windows-Installations-CD/DVD enthält, als Remote Storage (siehe Seite 127).
- Klicken Sie auf *Installation starten*.

  Alle Installationsdateien werden auf den verwalteten Server kopiert.

  In einem Bestätigungsdialog informiert Sie der Installation Manager über den Abschluss des Kopiervorgangs und fordert Sie auf, vor dem automatischen Neustart des verwalteten Servers alle Speichermedien aus den Wechsellaufwerken zu entfernen.

  Insbesondere müssen Sie vor dem Neustart des Systems auch alle aktiven Remote Storage-Verbindungen trennen.

- Trennen Sie vor dem Neustart des Systems die aktuellen Remote Storage-Verbindungen.

  Verfahren Sie hierfür wie folgt:

  - Starten Sie Remote Storage (siehe Seite 120).

    Es wird die Dialogbox *Storage Devices* mit den aktuell verbundenen Speichermedien und dem Hinweis auf „Safe Remove“ angezeigt.

  - Führen Sie einen „Safe Remove“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.
  - Klicken Sie auf *Disconnect...*, um alle Remote Storage-Verbindungen zu trennen.

► Klicken Sie im Bestätigungsdialog r auf *Ok*, um den verwalteten Server neu zu starten.

Nach dem Neustart des verwalteten Servers können Sie komplette Installation mithilfe der AVR überwachen.

Bei einer Windows-Installation von der Windows Installations-CD/DVD:

Für eine einwandfreie Synchronisation der Mauszeiger müssen Sie auf dem verwalteten Server nach Abschluss der Betriebssystem-Installation folgende Einstellungen anpassen:

– Geschwindigkeit des Mauszeigers
– Hardwarebeschleunigung

Wie Sie dabei im Einzelnen vorgehen, ist beschrieben im Abschnitt "Verwalteter Windows Server: Einstellungen für Mauszeiger-Synchronisation anpassen" auf Seite 102.

Bei einer Windows-Installation mithilfe des Installation Managers ist die einwandfreie Synchronisation der Mauszeiger automatisch gewährleistet.

11.4.2 Linux nach Konfiguration auf dem verwalteten Server installieren

Die Maus kann während der Linux-Installation verwendet, aber nicht synchronisiert werden.

Bei jedem Wechsel eines Remote Storage-Speichermediums müssen Sie die Remote Storage-Verbindung des aktuell verbundenen Mediums trennen und anschließend das neue Medium als Remote Storage verbinden.

Nach Abschluss der Konfiguration zeigt der Installation Manager folgenden Dialog an:

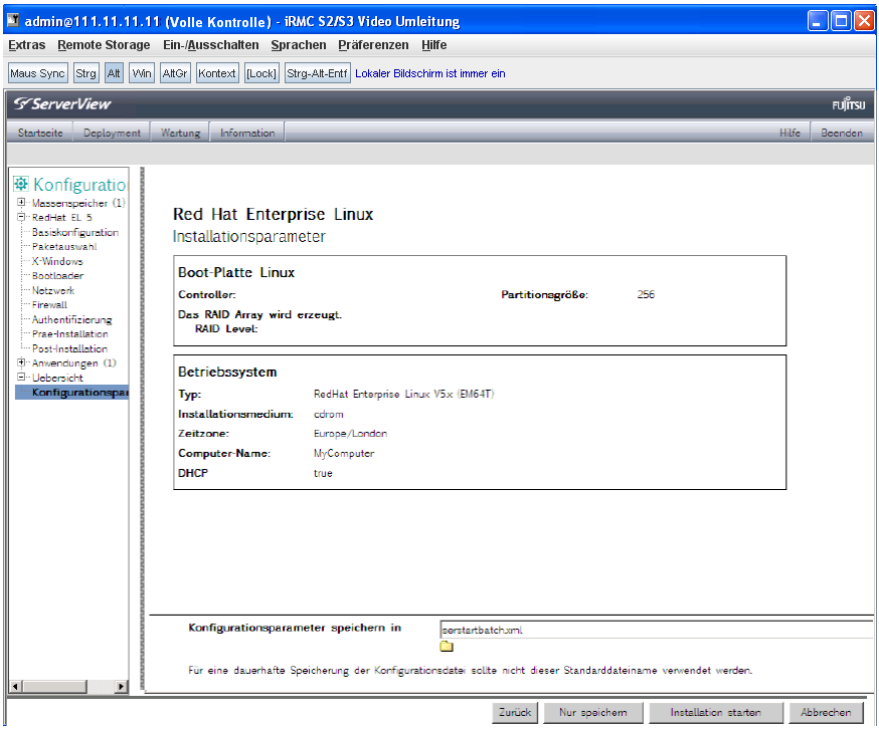


Bild 225: Installation Manager - Installation starten

Wenn Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers konfiguriert haben, gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- Trennen Sie Ihre zurzeit aktiven Remote Storage-Verbindungen. Näheres zum Trennen von Remote Storage-Verbindungen finden Sie auf Seite 131.
- Entfernen Sie die ServerView Suite DVD 1 aus dem DVD-ROM-Laufwerk am Remote-Arbeitsplatz.
- Legen Sie die Linux-Installations-CD/DVD in dieses DVD-ROM-Laufwerk ein.

  Schließen Sie die Anwendung, falls *autostart* aktiviert ist.

- Verbinden Sie das CD-ROM/DVD-ROM-Laufwerk, das die Linux-Installations-CD/DVD enthält, als Remote Storage (siehe Seite 127).
- Klicken Sie auf *Installation starten*.

  Alle Installationsdateien werden auf den verwalteten Server kopiert.

  In einem Bestätigungsdialog informiert Sie der Installation Manager über den Abschluss des Kopiervorgangs und fordert Sie auf, vor dem automatischen Neustart des verwalteten Servers alle Speichermedien aus den Wechsellaufwerken zu entfernen.

  Insbesondere müssen Sie vor dem Neustart des Systems auch alle aktiven Remote Storage-Verbindungen trennen.

- Trennen Sie vor dem Neustart des Systems die aktuellen Remote Storage-Verbindungen.

  Verfahren Sie hierfür wie folgt:

  - Starten Sie Remote Storage (siehe Seite 120).

    Es wird die Dialogbox *Storage Devices* mit den aktuell verbundenen Speichermedien und dem Hinweis auf „Safe Remove“ angezeigt.

  - Klicken Sie auf *Disconnect...*, um alle Remote Storage-Verbindungen zu trennen.
  - Führen Sie einen „Safe Remove“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.

- Klicken Sie im Bestätigungsdialog auf *Ok*, um den verwalteten Server neu zu starten.

Nach dem Neustart des verwalteten Servers können Sie komplette Installation mithilfe der AVR überwachen.

Für eine einwandfreie Synchronisation der Mauszeiger müssen Sie auf dem verwalteten Server nach Abschluss der Betriebssystem-Installation die erforderlichen Einstellungen anpassen. Wie Sie dabei im Einzelnen vorgehen, ist beschrieben im Abschnitt "Verwalteter Linux Server: Einstellungen für Mauszeiger-Synchronisation anpassen" auf Seite 105.

12 Anhang

Der Anhang informiert über folgende Themen:

– "Vom iRMC S2/S3 unterstützte IPMI OEM-Kommandos" on page 403

– "iRMC S2/S3 mit SCCI und per Script-Konfiguration konfigurieren" on page 431

12.1 Vom iRMC S2/S3 unterstützte IPMI OEM-Kommandos

Dieser Abschnitt beschreibt eine Auswahl der vom iRMC S2/S3 unterstützten OEM-spezifischen IPMI-Kommandos.

12.1.1 Überblick

Folgende IPMI OEM-Kommandos werden vom iRMC S2/S3 unterstützt:

- SCCI-konforme Power On/Off-Kommandos
  (SCCI: **S**erverView **C**ommon **C**ommand **I**nterface)
  - 0115 Get Power On Source
  - 0116 Get Power Off Source
  - 011C Set Power Off Inhibit
  - 011D Get Power Off Inhibit
  - 0120 Set Next Power On Time
- **SCCI-konforme Kommunikationskommandos**
  - 0205 System OS Shutdown Request
  - 0206 System OS Shutdown Request and Reset
  - 0208 Agent Connect Status
  - 0209 Shutdown Request Cancelled
- **SCCI-konforme Signalkommandos**
  - 1002 Write to System Display

- **Firmware-spezifische Kommandos**
  - 2004 Set Firmware Selector
  - 2005 Get Firmware Selector
  - C019 Get Remote Storage Connection
  - C01A Set Video Display on/off
- **BIOS-spezifisches Kommando**
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC S2/S3-spezifische Kommandos**
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F542 Get HDD lightpath status (Component Status Signal Read)
  - F543 Get SEL entry long text
  - F545 Get SEL entry text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Set Nonvolatile Cfg Memory to Default Values
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

12.1.2 Beschreibung der IPMI OEM-Kommandos

Nachfolgend sind die OEM-spezifischen IPMI-Kommandos im Einzelnen beschrieben.

12.1.2.1 Beschreibungsformat

Die OEM-spezifischen IPMI-Kommandos dieses Kapitels sind in dem Format beschrieben, das der IPMI-Standard für die Beschreibung der IPMI-Kommandos verwendet.

Der IPMI-Standard beschreibt die IPMI-Kommandos in Form von Kommando-Tabellen, in denen die Eingabe- und Ausgabeparameter des betreffenden Kommandos aufgelistet sind.

Informationen zu den IPMI-Standards finden Sie im Internet:

http://developer.intel.com/design/servers/ipmi/index.htm

12.1.2.2 SCCI-konforme Power On/Off-Kommandos

01 15 - Get Power On Source

Dieses Kommando informiert über die Ursache des zuletzt durchgeführten „Power On“. Die möglichen Ursachen werden nachfolgend aufgeführt.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**15** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	3	**01** Data Length
	4	Power on Source: Ursache des letzten Power On

Power On Source	Bedeutung
0x00	Software oder Kommando
0x01	Netzschalter (auf der Frontseite des Servers oder auf der Tastatur)
0x02	Automatischer Restart nach Stromausfall
0x03	Uhr oder Timer (Hardware Real-Time Clock (RTC) oder Software Timer)
0x04	Automatischer Restart nach Shutdown aufgrund eines Lüfterausfalls
0x05	Automatischer Restart nach Shutdown aufgrund kritischer Temperatur
0x08	Reboot nach Watchdog Timeout
0x09	Einschalten vom Remote-Arbeitsplatz aus (Modem RI Line, SCSI Termination Power, LAN, Chip-Kartenleser usw.)
0x0C	Reboot nach CPU-Fehler
0x15	Reboot durch Hardware-Reset
0x16	Reboot nach Warmstart
0x1A	Eingeschaltet durch ein Ereignis (Event) des PCI BUS Power Management
0x1D	Eingeschaltet via Remote Manager vom Remote-Arbeitsplatz aus
0x1E	Reboot/Reset via Remote Manager vom Remote-Arbeitsplatz aus

01 16 - Get Power Off Source

Dieses Kommando informiert über die Ursache des zuletzt durchgeführten „Power Off“. Die möglichen Ursachen werden nachfolgend aufgeführt.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**16** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	3	**01** Data Length
	4	Power off Source: Ursache des letzten Power Off

Power Off Source	Bedeutung
0x00	Software (SWOFF, SE: Power OFF per Kommando)
0x01	Netzschalter (auf der Frontseite des Servers oder auf der Tastatur)
0x02	Stromausfall
0x03	Uhr oder Timer (Hardware Real-Time Clock (RTC) oder Software Timer)
0x04	Lüfterausfall
0x05	Kritische Temperatur
0x08	Finales Ausschalten nach wiederholtem Watchdog Timeout
0x0C	Finales Ausschalten nach wiederholtem CPU-Fehler
0x1D	Ausgeschaltet via Remote Manager vom Remote-Arbeitsplatz aus

01 1C - Set Power Off Inhibit

Dieses Kommando setzt das *Power Off Inhibit*-Flag, mit dem ein willkürliches Ausschalten des Servers temporär verhindert werden kann.

Bei gesetztem *Power Off Inhibit*-Flag speichert die Firmware die Ursache für einen willkürlich versuchten "Power Off", "Power Cycle" oder Server-Neustart, führt die entsprechende Aktion jedoch nicht aus. Aktuell gespeichert wird dabei immer die Ursache für den zuletzt initiierten "Power Off"-, "Power Cycle"- oder Neustart-Versuch. Die gespeicherte Aktion wird erst nach dem Rücksetzen des *Power Off Inhibit*-Flags ausgeführt.

Das *Power Off Inhibit*-Flag wird nach einem Stromausfall oder bei Betätigung der Reset-Taste automatisch zurückgesetzt.

In seiner Wirkung entspricht das *Power Off Inhibit*-Flag dem Dump-Flag, das bei Erstellen eines Hauptspeicher-Dumps benutzt wird. Hier muss der Initiator vor dem Ziehen des Dumps das Flag setzen und nach Dump-Erstellung wieder zurücksetzen.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**1C** Command Specifier
	5	**00** Object ID
	6:7	**00 00** Value ID
	8	**01** Data Length
	9	Power Off Inhibit-Flag: 0 no Inhibit, 1 Inhibit
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first

01 1D - Get Power Off Inhibit

Dieses Kommando ermittelt den Wert des *Power Off Inhibit*-Flags.

Weitere Informationen zum *Power Off Inhibit*-Flag finden Sie in der Beschreibung zu "01 1C - Set Power Off Inhibit" on page 408.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**1D** Command Specifier
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**01** Response Data Length
	6	Power Off Inhibit-Flag: 0 no Inhibit, 1 Inhibit

01 20 - Set Next Power On Time

Dieses Kommando veranlasst das Einschalten des Systems zum spezifizierten Zeitpunkt, unabhängig von den im Configuration Space konfigurierten Ein-/Ausschalt-Zeiten.

Das Kommando bewirkt nur ein einmaliges Ausschalten

Eine zuvor per 01 20-Kommando festgelegte "Power On"-Zeit annullieren Sie, indem Sie mit einem nachfolgenden 01 20-Kommando die Power On-Zeit "0" spezifizieren.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**01** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**20** Command Specifier
	5	**00** Object ID
	6:7	**00 00** Value ID
	8	**04** Data Length
	9:12	Time (LSB first) (siehe unten)
Response Data	-	**BC**
	-	**01**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

Time (LSB first)

Zeitpunkt, dargestellt im UNIX-spezifischen Format, zu dem der Server sich wieder einschalten soll. Die Zeitangabe wird NICHT nicht-flüchtig gespeichert. Die Auflösung beträgt 1 Minute. Nach Einschalten des Servers zum spezifizierten Zeitpunkt wird die Zeitangabe intern auf 0 gesetzt.

Bei Angabe Time == 0 wird der Server nicht eingeschaltet.

12.1.2.3 SCCI-konforme Kommunikationskommandos

Die SCCI-konformen Kommunikationskommandos setzen voraus, dass der Agent-Service unter dem Server-Betriebssystem läuft. Für die Ausführung der Kommandos kommuniziert der iRMC S2/S3 mit dem SCCI-Agenten, der die Aktion dann ausführt.

02 05 - System OS Shutdown Request

Dieses Kommando initiiert den Shutdown des Server-Betriebssystems.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**05** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

02 06 - System OS Shutdown Request and Reset

Dieses Kommando initiiert den Shutdown des Server-Betriebssystems und den anschließenden Neustart des Systems.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**06** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

02 08 - Agent Connect Status

Dieses Kommando prüft, ob der SCCI-Agent aktiv ist.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**08** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	5	**01** Data Length
	6	**Connect Status:** 00: Verbindung verloren, keine Verbindung zum Agenten. 01: Verbindung wiederhergestellt, Verbindung zum Agenten existiert.

02 09 - Shutdown Request Cancelled

Dieses Kommando annulliert einen aktuellen Shutdown-Request.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**02** Cmd : Command Group Communication
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**09** Command Specifier
Response Data	-	**BC**
	-	**02**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

12.1.2.4 SCCI-konformes Signalkommando

10 02 - Write to System Display

Dieses Kommando gibt Text auf ein angeschlossenes LocalView Display aus.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**10** Cmd : Command Group Fan Test
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**02** Command Specifier
	5	**Object Index**: : Zeile auf dem Display, in die geschrieben werden soll.
	6:7	**Value ID** (nicht verwendet)
	8	**Length** Anzahl der zu schreibenden Zeichen + 1. (Der String braucht nicht durch das NULL-Byte terminiert zu sein. Falls die Länge des Displays für die Darstellung des Strings nicht ausreicht, werden überzählige Zeichen abgeschnitten.)
	9	**Attribut:** 0 = String linksbündig schreiben 1 = String zentriert schreiben
	10:10+n	**Zeichen**, die auf das Display geschrieben werden sollen. Der String braucht nicht durch das NULL-Byte terminiert zu sein.
Response Data	-	**BC**
	-	**10**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

12.1.2.5 Firmware-spezifische Kommandos

20 04 - Set Firmware Selector

Dieses Kommando konfiguriert, welches Firmware Image des iRMC S2/S3 nach einem Firmware-Reset aktiv ist.

Request Data	-	**20** NetFnlLUN: Firmware
	-	**04** CMD : Command Group Firmware
	1	Selector: 0 = Auto (Firmware Image mit der neuesten Firmware-Version.) 1 = low firmware image 2 = high firmware image 3 = Auto oldest version (Firmware Image mit der ältesten Firmware-Version.) 4 = MRP (Firmware Image mit der zuletzt aktualisierten Firmware) 5 = LRP (Firmware Image mit der am längsten nicht mehr aktualisierten Firmware)
Response Data	-	**24**
	-	**04**
	1	Completion Code

20 05 - Get Firmware Selector

Dieses Kommando liefert die Einstellungen des aktuellen Firmware Selectors .

Request Data	-	**20** NetFnlLUN: Firmware
	-	**05** CMD : Command Group Firmware
Response Data	-	**24**
	-	**05**
	1	Completion Code
	2	Next Boot Selector: 0 = Auto (Firmware Image mit der neuesten Firmware-Version) 1 = low EEPROM 2 = high EEPROM 3 = Auto oldest version (EEPROM mit der ältesten Firmware-Version) 4 = MRP (Firmware Image mit der zuletzt aktualisierten Firmware) 5 = LRP (Firmware Image mit der am längsten nicht mehr aktualisierten Firmware)
	3	Running Selector; zeigt an, welcher EEPROM aktiv ist: 1 = low EEPROM 2 = high EEPROM

C0 19 - Get Remote Storage Connection or Status

Dieses Kommando informiert je nach Parametrisierung,

– ob Remote Storage-Verbindungen bestehen,
– über Status und Typ der Remote Storage-Verbindung(en).

Wenn *Request Data 1* auf "1" gesetzt ist, informiert das Kommando, ob Speichermedien als Remote Storage verbunden sind.

Request Data	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : Command Group Firmware
	1	01
	2	00
	3	00
Response Data	-	**C4**
	-	**19**
	1	Completion Code
	2	**01**
	3	**00: No** **01: Ja, verbunden**
	4	**00**
	5	**00**

Wenn *Request Data 1* auf "2" gesetzt ist, informiert das Kommando über Status und Typ der Remote Storage-Verbindung(en).

Request Data	-	**C0** NetFnlLUN: OEM
	-	**19** CMD : Command Group Firmware
	1	02
	2	00
	3	00 = Connection 0 01 = Connection 2
Response Data	-	**C4**
	-	**19**
	1	Completion Code
	2	**02**
	3	**00**
	4	**00**
	5	**00 = Invalid / unknown** **01 = idle** **02 = Connection Attempt pending** **03 = Connected** **04 = Connection Attempts retries exhausted / failed** **05** = **Connection lost** **06** = **Disconnect pending**
	6	00 **= Invalid / unknown** **01 = Storage Server / IPMI** **02 = Applet** **03 = None / Not connected**

C0 1A - Set Video Display On/Off

Dieses Kommando ermöglicht das Ein- und Ausschalten der lokalen Konsole.

Request Data	-	**C0** NetFnlLUN: OEM
	-	**1A** Cmd : Command Group Fan Test
	1	00 = Set Video Display On 01 = Set Video Display Off
Response Data	-	**C4**
	-	**1A**
	1	Completion Code

12.1.2.6 BIOS-spezifische Kommandos

F1 09 - Get BIOS POST State

Dieses Kommando informiert, ob sich das BIOS in der POST-Phase befindet.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**09** Command Specifier
Response Data	-	**BC**
	-	**F1**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	[7:1] - reserved [0] - BIOS POST State : 0 = BIOS is not in POST 1 = BIOS is in POST

F1 15 - Get CPU Info

Dieses Kommando liefert CPU-interne Informationen. Der iRMC S2/S3 empfängt diese Information während der POST-Phase das BIOS.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F1** Cmd : Command Group BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**15** Command Specifier
	5	Socket Number (0-based) of the CPU
Response Data	-	**BC**
	-	**F1**
	1	**Completion Code:** 01 = Unpopulated CPU Socket
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	CPU ID, LS Byte first
	7	Platform ID
	8	Brand ID
	9:10	Maximal Core Speed of the CPU [MHz], LS Byte first
	11:12	Intel Qickpath Interconnect in Mega Transactions per second, LS Byte first
	13	T-Control Offset
	14	T-Diode Offset
	15	CPU data Spare
	16:17	Record ID CPU Info SDR, LS Byte first
	18:19	Record ID Fan Control SDR, LS Byte first
	20:21	CPU ID High Word, LS Byte first (0 if none)

12.1.2.7 iRMC S2/S3-spezifische Kommandos

F5 10 - Get System Status

Dieses Kommando liefert eine Vielzahl interner Informationen über den Server, wie z. B. Power- oder Fehlerstatus.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Memory
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**10** Command Specifier
	5:8	**Timestamp**
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	5	**System Status** (Details siehe unten.)
	6	**Signaling** (Details siehe unten.)
	7	**Notifications** (Details siehe unten.)
	8	**POST Code**

Der Zeitstempel (Timestamp) wird nur für die Auswertung des *Notifications*-Byte benötigt.

System Status

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

Signaling

Bit 7 - Localize LED

Bit 6 -

Bit 5 -

Bit 4 -

Bit 3 - CSS LED

Bit 2 - CSS LED

Bit 1 - Global Error LED

Bit 0 - Global Error LED

Notifications

Bit 7 - SEL Modified (New SEL Entry)

Bit 6 - SEL Modified (SEL Cleared)

Bit 5 - SDR Modified

Bit 4 - Nonvolatile IPMI Variable modified

Bit 3 - ConfigSpace Modified

Bit 2 -

Bit 1 -

Bit 0 - New Output on LocalView panel

F5 12 - Get EEPROM Version Info

Dieses Kommando informiert über die aktuellen Versionen von Bootloader, Firmware und SDR in den EEPROMs.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group Memory
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**12** Command Specifier
	5	EEPROM# 00=EEPROM 1; 01=EEPROM 2
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	5	**Status** 00=Checksum Error Runtime FW, 01=OK
	6	**Major FW Revision** Binary coded
	7	**Minor FW Revision** BCD coded
	8:10	**Aux. FW Revision** Binary coded (major/minor/res.)
	11	**Major FW Revision** ASCII coded letter
	12	**Major SDRR Revision** BCD coded
	13	**Minor SDRR Revision** BCD coded
	14	**SDRR Revision Char.** ASCII coded letter
	15	**SDRR-ID** LSB binary coded
	16	**SDRR-ID** MSB binary coded
	17	**Major Booter Revision** Binary coded
	18	**Major Booter Revision** BCD coded
	19:20	*Aux. Booter Revision* Binary coded (major/minor)

F5 42 - Get HDD lightpath status (Component Status Signal Read)

Dieses Kommando gibt Informationen zum Status des Festplatten-Steckplatzes (HDD) zurück.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**42** Command Specifier
	5	**Entity ID** (*Tabelle 37-12* in der IPMI 1.5 Spez.) der Komponente, dessen Statussignal gelesen werden soll.
	6	**Entity Instance** (0-basiert) der Komponente, dessen Statussignal gelesen werden soll.
	7	**Sensor Type** (*Tabelle 36-3* der IPMI-Spez.) des Sensors, der den Status der Komponente meldet, der das Statussignal zugeordnet wird.
	(8)	Option (optional) Bit 7:2 - Reserved Bit 1 :Completion Code 0x02 suppressed Bit 0 - 1 : Return ID String of Component Status Sensor
Response Data	-	**BC**
	-	**F5**
	1	**Completion Code:** 01= Statussignal nicht verfügbar 02 = Komponente nicht vorhanden
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5	**Signalstatus:** 00 = OK 01 = Identifizierung 02 = Prefailure-Warnung 03 = Fehler
	6	**CSS und physische LED verfügbar:** Bit 6:0 - 0 = keine physische LED verfügbar Bit 6:0 > 00 = Physische LED verfügbar; ein- oder mehrfarbig, Code Bit 7 = 0: Keine CSS-Komponente Bit 7 = 1: CSS-Komponente
	(7)	Länge des ID-Strings des Komponenten-Status-Sensors (nur vorhanden, wenn Bit 0 in Request Byte 8 festgelegt wurde)

(8 .. m)	Länge des ID-Strings des Komponenten-Status-Sensors in ASCII-Zeichen (nur vorhanden, wenn Bit 0 in Request Byte 8 festgelegt wurde)

F5 43 - Get SEL entry long text

Dieses Kommando übersetzt einen vorliegenden System Event Log (SEL) in Klartext.

Request Data	-	**B8** NetFn|LUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**43** Command Specifier
	5:6	**Record ID** des SEL-Datensatzes, LS Byte first 0x0000: ersten Datensatz abrufen 0xFFFF: letzten Datensatz abrufen
	7	**Offset** als Antwort auf SEL-Text
	8	**MaxResponseDataSize** Größe von *Konvertierte SEL-Daten* (16:n) als Antwort
Response Data	-	**BC**
	-	**F5**
	1	Completion Code:
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	Next Record ID
	7:8	**Actual Record ID**
	9	**Record type**
	10:13	**Timestamp**
	14	**Severity:** Bit 7: 0 = No CSS component 1 = CSS component Bit 6-4: 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown' Bit 3-0: reserved, read as 0000
	15	**Länge der Daten** des gesamten Texts
	16:n	**Konvertierte SEL-Daten** angefordertes Teil (n = 16 + MaxResponseDataSize - 1)
	n + 1	**String Terminator** nachfolgendes '\0'-Zeichen

F5 45 - Get SEL entry text

Dieses Kommando übersetzt einen vorliegenden Fehlerspeicher (System Event Log, SEL) in ASCII-Text.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	4	**45** Command Specifier
	5:6	**Record ID** von SDR, LS Byte first
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte first
	5:6	**Next Record ID**
	7:8	**Actual Record ID**
	9	**Record type**
	10:13	**Timestamp**
	14	**Severity:** Bit 7: 0 = No CSS component 1 = CSS component Bit 6-4: 000 = INFORMATIONAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown' Bit 3-0: reserved, read as 0000
	15	**Data length**
	16:35	**Converted SEL data**

F5 B0 - Set Identify LED

Mithilfe dieses Kommandos können Sie die Identifizierungs-LED (blau) des Servers ein- und ausschalten. Darüber hinaus können Sie die GPIOs festlegen und lesen, die direkt mit der Identify LED verbunden sind.

Die Identify LED können Sie außerdem über den Identify Button am Servers ein- und ausschalten.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**B0** Command Specifier
	5	**Identify LED:** 0: Identify LED aus 1: Identify LED ein
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

F5 B1 - Get Identify LED

Dieses Kommando informiert über den Status der Identify-LED (blau) des Servers.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**B1** Command Specifier
Response Data	-	**BC**
	-	F5
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	5	Status der Identify LED (nur Bit 0 ist relevant)

F5 B3 - Get Error LED

Dieses Kommando informiert über den Status der Global Error LED (rot) und der CSS LED (gelb) des Servers. Die Global Error LED zeigt die schwerwiegendsten Fehler-Status der Komponenten an. Die CSS LED zeigt an, ob Fehler vorliegen, die Sie als Kunde selber beheben können.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**B3** Command Specifier
Response Data	-	BC
	-	F5
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	5	**Fehlerstatus-LED:** 0 : CSS ausgeschaltet/GEL ausgeschaltet 1 : CSS ausgeschaltet/GEL eingeschaltet 2 : CSS ausgeschaltet/GEL blinkt 3 : CSS eingeschaltet/GEL ausgeschaltet 4 : CSS eingeschaltet/GEL eingeschaltet 5 : CSS eingeschaltet/GEL blinkt 6 : CSS blinkt/GEL ausgeschaltet 7 : CSS blinkt/GEL eingeschaltet 8 : CSS blinkt/GEL blinkt

F5 DF - Reset Nonvolatile Cfg Variables to Default

Dieses Kommando setzt alle nicht-flüchtigen IPMI Settings auf Default-Werte.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**DF** Command Specifier
	5:8	43 4C 52 AA = 'CLR'0xaa: Sicherheitscode
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

F5 E0 - Reset ConfigSpace Variables to Default

Dieses Kommando setzt alle Variablen des Configuration Space auf Default-Werte.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**E0** Command Specifier
	5:8	43 4C 52 AA = 'CLR'0xaa: Sicherheitscode
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

F5 F8 - Delete User ID

Das System unterstützt bis zu 16 Benutzer. Mit diesem Kommando können Sie iRMC S2/S3-Benutzerkennungen löschen.

ACHTUNG!

Wenn Sie alle Benutzerkennungen löschen, kann der iRMC S2/S3 nicht mehr bedient werden.

Request Data	-	**B8** NetFnlLUN: OEM/Group
	-	**F5** Cmd : Command Group BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First
	4	**F8** Command Specifier
	5:8	User ID (1-16)
Response Data	-	**BC**
	-	**F5**
	1	Completion Code
	2:4	**80 28 00** IANA-Enterprise-Number FTS, LS Byte First

12.2 iRMC S2/S3 mit SCCI und per Script-Konfiguration konfigurieren

Der vorliegende Abschnitt informiert über folgende Themen:

– Verwenden einer SCCI-konformen (**S**erverView **C**ommon **C**ommand **I**nterface) Schnittstelle zum Konfigurieren des iRMC S2/S3.

– Script-Konfiguration des iRMC S2/S3

12.2.1 iRMC S2/S3-Konfigurationsdaten

Beachten Sie, dass die nachfolgend beschriebene Schnittstelle hauptsächlich für eine Remote-Konfiguration gilt und **keine** SCCI-Implementierung ist. Es werden nur die SCCI-Kommando- und -Konfigurationsdefinitionen und das SCCI-Dateiformat verwendet.

12.2.1.1 Überblick

Das iRMC S2/S3 speichert interne Konfigurationsdaten in zwei separaten Abschnitten des NVRAM (Non-Volatile RAM):

– FTS-spezifische ConfigSpace-Daten, die von der Firmware über eine festgelegte interne Tabelle mit Beschreibungen aufgerufen werden.

– Ursprüngliche, herstellerspezifische NVCFG-Daten, auf die von den Offset-Definitionen zugegriffen wird.

Einige Konfigurationsdaten der ursprünglichen NVCFG-Daten werden intern von der Firmware zugeordnet, damit mithilfe von ConfigSpace-Zugriffsmethoden darauf zugegriffen werden kann. Der Zugriff auf DNS-Server und die DNS-Konfiguration des iRMC S2/S3 ist über IPMI OEM LAN-Konfigurationsparameter und über ConfigSpace möglich. Mit beiden Methoden wird auf die gleichen Datenstrukturen der unteren Stufe im Original-NVCFG-Abschnitt zugegriffen.

Nicht-iRMC S2/S3-spezifische ServerView-Softwarekomponenten (z. B. die ServerView-Agenten oder der Server Configuration Manager) ordnen in manchen Fällen auch Standard-IPMI-verwandte Kommandos und Konfigurationselemente zu, z. B. Standard-IPMI-Benutzerkonfiguration oder IPv4-Netzwerkkonfiguration. Dadurch wird eine Abstraktionsebene zwischen der IPMI BMC-Ebene und höheren Softwareebenen implementiert.

Das SCCI ist eine generische Anwendungsprogrammierschnittstelle (API), die von Fujitsu für verschiedene Server Management Controller-Hardware sowie Server Management-Software (z. B. ServerView-Agenten) definiert wird. Sie kann mühelos erweitert werden, um neue Kommandos oder neue Konfigurationselemente zu umfassen. Eine Architekturübersicht des SCCI finden Sie in der Online-Hilfe für die ServerView-Agenten.

Ab iRMC S2 Firmware 5.20A (IPv6-Version) unterstützt iRMC S2/S3 die Remote-Konfiguration und begrenztes Scripting über die */config URL* im iRMC S2/S3.

Vorteile einer iRMC S2/S3-Remote-Konfiguration über einen webbasierten Zugriff

Die Remote-Konfiguration von iRMC S2/S3 über einen webbasierten Zugriff bietet die folgenden Vorteile:

– Verwendet die HTTP POST-Operation zum Hochladen von Dateien in das iRMC S2/S3. Es sind keine speziellen Tools erforderlich. Jedes allgemeine Tool oder jede Scriptumgebung, die authentifizierte HTTP POST-Operationen unterstützen, können verwendet werden. Beispiel-Skripte befinden sich auf der ServerView Suite DVD 1.

– Verwendet integrierte Authentifizierungs- und Autorisierungsmethoden des iRMC S2/S3-Webservers.

– Unterstützt die HTTP 1.1 Basic- und Digest-Authentifizierung basierend auf RFC 2617 mit lokalen iRMC S2/S3-Benutzerkonten.

– Bietet optional integrierte leistungsstarke Verschlüsselung mit standardmäßig HTTPS-basiertem Zugriff.

– Kann mit globalen Benutzerkonten (verwaltet durch einen LDAP-Verzeichnisdienst) und HTTP 1.1 Basic-Authentifizierung verwendet werden.

Wenn die HTTP 1.1 Basic-Authentifizierung verwendet wird, wird aus Verschlüsselungs- und Vertraulichkeitsgründen empfohlen, das HTTPS-Protokoll zu verwenden, um die Benutzername-Kennwort-Kombination zu schützen.

– Verwendet ein auf XML basierendes Konfigurationsdateiformat. Sie haben die Möglichkeit, die Datei manuell zu bearbeiten oder sie aus einer Referenzinstallation oder dem Server Configuration Manager zu exportieren.

  Die Konfigurationsdatei kann mit anderen SCCI-basierten Installationsmethoden (z. B. Server Configuration Manager) erneut verwendet werden.

– Es ist eine mühelose Erweiterung auf neue Konfigurationselemente und neu unterstützte SCCI-Kommandos möglich.

12.2.1.2 SCCI-Dateiformat

Das Format der verwendeten XML-Konfigurationsdatei (*.pre*) stammt aus der Setup-Konfigurationshilfedatei, die zusammen mit den ServerView-Agenten unter Windows installiert wird. Eine Kopie dieser Beschreibung mit iRMC S2/S3-spezifischen Hinweisen wird unten aufgeführt.

Die Konfigurationsdatei basiert auf einer XML-Syntax:

– Jede Konfigurationseinstellung besteht aus einem einfachen XML-Fragment, das mit einem „<CMD>“-Tag beginnt.

– Die vollständige Sequenz der Konfigurationseinstellungen befindet sich zwischen dem Tag-Paar „<CMDSEQ>“ und „</CMDSEQ>“.

Im Folgenden finden Sie ein Beispiel für eine typische Kommandosequenz mit zwei Konfigurationseinstellungen:

```
<CMDSEQ>
<CMD Context="SCCI" OC="ConfigSpace" OE="3800" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">04</DATA>
<CMD Context="SCCI" OC="ConfigSpace" OE="3801" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">00</DATA> </CMD>
</CMDSEQ>
```

Der Parameter *Context* wird intern zur Auswahl des Anbieters der Operation verwendet. Derzeit ist `SCCI` der einzige unterstützte Anbieter.

Parameter von SCCI-Anbieter-spezifischen Kommandos

Die folgenden SCCI-Anbieter-spezifischen Kommandos stehen zur Verfügung:

Operationscode (`OC`)
: Hexadezimalwert oder String, der das Kommando bzw. den Operationscode festlegt.

  > **i** Das iRMC S2/S3 unterstützt nur einen eingeschränkten Satz an SCCI-Kommandos. Eine Liste der unterstützten Kommandos finden Sie unter table "Vom iRMC S2/S3 unterstützte SCCI-Kommandos" on page 439

Operationscode-Erweiterung (`OE`)
: Hexadezimalwert für erweiterten Operationscode. Standard: `OE=0`

  Bei ConfigSpace-Lese-/Schreibvorgängen definiert dieser Wert die ConfigSpace-ID.

Objektindex (`OI`)
: Hexadezimalwert zur Auswahl einer Objektinstanz. Standard: OI=0"

Operationscode-Typ (`Type`)
: Bei Konfigurationseinstellungen werden die Werte `GET` (Lesevorgang) und `SET` (Schreibvorgang) unterstützt. Standard: Type=GET

  > **i** Bei `SET`-Operationen sind Daten erforderlich. Verwenden Sie zum Angeben des entsprechenden Datentyps den unten beschriebenen Parameter *Data (DATA)*.

Gehäuse-ID (`CA`)
: Ermöglicht es Ihnen, ein Erweiterungsgehäuse auszuwählen und die Gehäuse-ID zu verwenden.

  > **i** Verwenden Sie diesen Parameter **nicht**, um das Systemgehäuse anzufordern!

Daten (DATA)

Bei angegebenem SET-Parameter (Schreibvorgang): Datentyp (Type-Parameter) und, in einigen Fällen, Länge der Daten (LEN-Parameter) sind erforderlich.

Derzeit werden die folgenden Datentypen unterstützt:

– xsd::integer

  Ganzzahl

  Beispiel

  ```
  <DATA Type="xsd::integer">1234</DATA>
  ```

– xsd::hexBinary

  Byte-Stream. Jedes Byte wird mit zwei ASCII-Zeichen codiert. Verwenden Sie den Len-Parameter wie im unten stehenden Beispiel gezeigt, um die Länge des Streams festzulegen (d. h. die Anzahl der Bytes).

  Der Datentyp xsd::hexBinary kann ohne Einschränkung verwendet werden.

  Beispiel

  Ein Stream aus vier Bytes 0x00 0x01 0x02 0x04 wird als folgender ASCII-Stream codiert:

  ```
  <DATA Type="xsd::hexBinary" Len="4">0001020304</DATA>
  ```

– xsd::string

  Normalerweise zur Übertragung der Strings verwendet. Darüber hinaus kann der Typ string für IPv4-Adressen und MD5-basierte Benutzerkennwörter verwendet werden. In diesem Fall werden die String-Daten intern in das akzeptierte Zielformat konvertiert.

  Verschlüsselte Daten übertragen

  Eine Fujitsu-eigene Datenverschlüsselung wird bei einigen vertraulichen Daten unterstützt, z. B. Benutzer- oder Dienstzugriffskennwörter (LDAP/SMTP) oder für den AVR-Lizenzschlüssel von iRMC S2/S3. Mit dem Programm *iRMC_PWD.exe* können Sie Kennwortdaten verschlüsseln (siehe section "Verschlüsselte Kennwörter mit dem Programm iRMC_PWD.exe generieren" on page 443).

`Encrypted="1"` muss im Tag `<DATA>` festgelegt werden, um anzugeben, dass die zu schreibenden Daten verschlüsselt sind.

Beispiele

String „Hello World“ übertragen:

```
<DATA Type="xsd::string">Hello World</DATA>
```

Kennwort als reinen (lesbaren) Text übertragen:

```
<DATA Type="xsd::string">Eigenes lesbares
Kennwort</DATA>
```

Verschlüsseltes Kennwort übertragen:

```
<DATA Type="xsd::string"
Encrypted="1">TpVlTJwCyHEIsC8tk24ci83JuR9l</DATA>
```

Transferring the IPv4 address "192.23.2.4"

```
<DATA Type="xsd::string">192.23.2.4</DATA>
```

ACHTUNG!

Der Datentyp `xsd::string` ist auf lesbare Strings, IP-Adressen und MD5-basierte Benutzerkennwörter beschränkt.

Bei allen anderen Daten muss der Datentyp `xsd::hexbinary` verwendet werden.

Geben Sie die Zeichen ä, ö, ü usw. in Strings nicht direkt an, es sei denn, sie werden von der jeweiligen Anwendung benötigt.

Weder die SCCI- noch die ConfigSpace-Schnittstelle speichern Informationen zur Zeichencodierung. Daher werden alle Nicht-US-ASCII-Zeichen intern von der verwendenden Anwendung interpretiert und sollten vermieden werden.

Wenn Sie Sonderzeichen angeben müssen, stellen Sie sicher, dass Sie Ihre Datei im UTF-8-Format und mit dem korrekten BOM bearbeiten und speichern.

Kommandostatus (`Status`)

Nach der Übertragung der Konfigurationseinstellungen enthält der `Status` das Ergebnis der Operation. Wenn die Operation erfolgreich abgeschlossen wurde, wird der Wert `0` zurückgegeben.

Eine Spezifikation aller öffentlichen Konfigurationseinstellungen (ConfigSpace) finden Sie in der Datei *SCCI_CS.pdf* im Ordner *Help* des Installationspakets für ServerView-Agenten. Darüber hinaus wird die Datei *SCCI_CS.pdf* mit dem PRIMERGY Scripting Toolkit verteilt.

12.2.1.3 Einschränkungen

Alle in der *.pre*-Datei angegebenen Kommandos werden normalerweise in der angegebenen Reihenfolge ausgeführt. Die folgenden Ausnahmen weichen von dieser Regel ab:

– Um eine Unterbrechung der Netzwerkverbindung zu verhindern, werden Kommandos für die IPv4- und VLAN-Netzwerkkonfiguration am Ende einer Kommandosequenz ausgeführt.

– Die IPv6-Konfiguration ist derzeit auf die Konfiguration von nicht-flüchtigen IPv6-Konfigurationsparametern beschränkt.

  Als Workaround könnten Sie folgendermaßen vorgehen:

  1. Ordnen Sie das Script folgendermaßen an:

     a) Zu Beginn des Scripts: Deaktivieren Sie IPv6.

     b) Konfigurieren Sie IPv6-Parameter.

     c) Am Ende des Scripts: Aktivieren Sie IPv6.

  2. Übertragen Sie das Script von einer IPv4-Adresse.

– Das SSL-Zertifikat und der entsprechende passende private Schlüssel werden am Ende einer Kommandosequenz ausgeführt. Beide Komponenten müssen in der gleichen *.pre*-Datei angegeben sein und werden auf Übereinstimmung überprüft.

– Bei erforderlicher oder erwünschter Energieverwaltungsoperation für den verwalteten Server oder Neustart von iRMC S2/S3:

  Es wird empfohlen (es ist jedoch nicht erforderlich), dass Sie diese Kommandos in separaten Kommandodateien ausführen. Unterteilen Sie dazu beispielsweise die Konfigurations- und Energieverwaltungsvorgänge in separate Aufgaben.

– Optional müssen Zeitverzögerungen zwischen der Ausführung der aufeinander folgenden Kommandos außerhalb des Scripts implementiert werden.

  Dies können Sie folgendermaßen umsetzen:

  1. Unterteilen Sie das Script in angemessene separate Scripte.
  2. Verwenden Sie den Funktionsbereich des Clients, um Zeitverzögerungen zwischen dem Versenden der einzelnen Dateien einzufügen.

12.2.1.4 Konfigurationsdaten aus/auf iRMC S2/S3 exportieren/importieren

Über die Seite *Save iRMC S2/S3 Firmware Settings* in der iRMC S2/S3-Webschnittstelle können Sie die aktuellen iRMC S2/S3-Konfigurationsdaten in einer Konfigurationsdatei (*.pre*) speichern (exportieren). Zudem können Sie die iRMC S2/S3-Konfigurationsdaten aus einer bestehenden Konfigurationsdatei (*.pre*) importieren, d. h. die Konfigurationsdaten in das iRMC S2/S3 laden. (Details siehe section "iRMC S2/S3 Firmware Einstellungen abspeichern" on page 176.)

Zum Importieren einer iRMC S2/S3-Konfiguration können Sie alternativ die entsprechende SCCI-Kommando-Datei an die */config URI* des iRMC S2/S3 mittels einer HTTP POST-Operation senden.

12.2.2 Script-Konfiguration des iRMC S2/S3

Der vorliegende Abschnitt informiert über folgende Themen:

– Vom iRMC S2/S3 unterstützte SCCI-Kommandos

– Verwenden von verschiedenen Script-Sprachen für die Script-Konfiguration des iRMC S2/S3

– Generieren von verschlüsselten Kennwörtern mit dem Programm *iRMC_PWD.exe*

12.2.2.1 Liste der vom iRMC S2/S3 unterstützten SCCI-Kommandos

Die vom iRMC S2/S3 unterstützten SCCI-Kommandos finden Sie in table 19:

SCCI-Operationscode	SCCI-Kommando-String	Bedeutung
0xE002	ConfigSpace	ConfigSpace-Schreibvorgang
0x0111	PowerOnCabinet	Server einschalten
0x0112	PowerOffCabinet	Server ausschalten
0x0113	PowerOffOnCabinet	Server aus-/einschalten
0x0204	ResetServer	Hard-Reset des Servers
0x020C	RaiseNMI	NMI (Non Maskable Interrupt) auslösen
0x0205	RequestShutdownAndOff	System herunterfahren, Agent muss ausgeführt werden
0x0206	RequestShutdownAndReset	Systemneustart, Agent muss ausgeführt werden
0x0209	ShutdownRequestCancelled	Shutdown-Anforderung abbrechen
0x0203	ResetFirmware	BMC-Reset durchführen
0x0250	ConnectRemoteStorageServer	Standalone Remote Storage Server verbinden oder trennen

Table 19: Vom iRMC S2/S3 unterstützte SCCI-Kommandos

12.2.2.2 Scripte mit cURL

Das Open-Source-Kommandozeilen-Tool cURL ermöglicht es Ihnen, Daten mit einer URL-Syntax zu übertragen. Sie können die aktuelle Version des Quellcodes sowie vorab kompilierte Versionen für verschiedene Betriebssysteme unter *http://curl.haxx.se/* herunterladen.

Im Folgenden finden Sie einige Beispiele, wie Sie mit cURL eine Konfigurationsdatei an das iRMC S2/S3 senden können.

Details zu den cURL-Kommandozeilenoptionen finden Sie in der cURL-Dokumentation.

– HTTP-Zugriff mit Basic-Authentifizierung (Standard) und das standardmäßige iRMC S2/S3-Admin-Konto:

```
curl --basic -u admin:admin --data @Config.pre
http://<IP-Adresse des iRMC S2/S3>/config
```

– HTTP-Zugriff mit Digest-Authentifizierung und das standardmäßige iRMC-Admin-Konto:

```
curl --digest -u admin:admin --data @Config.pre
http://<IP-Adresse des iRMC S2/S3>/config
```

– HTTPS-Zugriff ohne Zertifikatsprüfung (-k) und Digest-Authentifizierung und das standardmäßige iRMC-Admin-Konto:

```
curl --digest -k -u admin:admin --data @Config.pre
https://<IP-Adresse des iRMC S2/S3>/config
```

– HTTPS-Zugriff mit einem LDAP-Benutzerkonto.

  Beachten Sie, dass Sie für LDAP-Benutzer die Basic-Authentifizierung angeben müssen.

```
curl --basic -k -u LDAPuser:LDAPpassword --data @Config.pre
https://<IP-Adresse des iRMC S2/S3>/config
```

12.2.2.3 Scripte mit Visual Basic (VB) Script

Mit dem folgenden VB-Script wird eine Konfigurationsdatei an das iRMC S2/S3 gesendet:

```
IP_ADDRESS = "<IP-Adresse des iRMC S2/S3>"
USER_NAME  = "admin"
PASSWORD   = "admin"

FILE_NAME  = ".\\ConfigFile.pre"

Const ForReading = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(FILE_NAME, ForReading)

' ---------------------------------------------------------------------
On Error Resume Next

Set xmlHttp = CreateObject("Microsoft.XMLHTTP")
xmlHttp.Open "POST", "http://" & IP_ADDRESS & "/config", False,
USER_NAME, PASSWORD
xmlhttp.setRequestHeader "Content-Type", "application/x-www-
form-urlencoded"
xmlHttp.Send objFile.ReadAll

Wscript.Echo xmlhttp.responsexml.xml
```

12.2.2.4 Scripte mit Python

```
#!/usr/bin/python3
import sys
import httplib2
from urllib.parse import urlencode

# ============================================================
# iRMC

USER = 'admin'
PWD  = 'admin'
IP_ADDR = '192.168.1.100'
# ============================================================

h = httplib2.Http()

# Basic/Digest authentication
h.add_credentials(USER, PWD)

def doit(data,ausgabe=sys.stdout):
  try:
    resp, content = h.request("http://%s/config" % IP_ADDR,
    "POST", data)
    if resp['status'] == '200'
      data = content.decode('utf-8')
      print(data,file=ausgabe)
      else:
      print('STATUS:',resp['status'],file=ausgabe)
      print(str(resp),file=ausgabe)
  except Exception as err:
    print('ERROR:',str(err),file=ausgabe)
  print()


# Beispiel 1 - Konfigurationsdatei an das iRMC S2/S3 senden
try:
  data = open('ConfigFile.pre').read()
  doit(data)
except Exception as err:
  print('ERROR:',str(err),file=ausgabe)


# Beispiel 2 - ConfigSpace-Werte festlegen
# 0x200 (ConfCabinetLocation) und
# 0x204 (ConfSystemContact) direkt aus Script
#
LocationContact = '''<?xml version="1.0" encoding="UTF-8"
standalone="yes" ?>
```

```
<CMDSEQ>
  <!-- ConfCabinetLocation -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="200" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
  <!-- ConfSystemContact -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="204" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
</CMDSEQ>
'''

doit(LocationContact % ("Ostsee","Kiel"))
```

12.2.2.5 Verschlüsselte Kennwörter mit dem Programm iRMC_PWD.exe generieren

Das Hilfsprogramm von Fujitsu Technology Solutions zur iRMC-Kennwortverschlüsselung und -prüfung *iRMC_PWD.exe* ist ein Win32-Programm, mit dem Sie verschlüsselte Kennwörter für SCCI-Scripte generieren können. Mit *iRMC_PWD.exe* können Sie ein einzelnes Kennwort verschlüsseln und eine SCCI-Batch-Datei für die Script-Konfiguration generieren.

iRMC_PWD Standard-Kommandozeilenoptionen

[-h] [-?]
: Diese Hilfe.

[-v]
: Überprüfen eines verschlüsselten Kennwort-Strings.

[-o] <oid>
: Die Objekt-ID für die zu verschlüsselnden Daten.

[-u] <username>
: Benutzername für die angegebene Objekt-ID (optional).

[-p] <password>
: Kennwort für die angegebene Objekt-ID / / zu prüfender verschlüsselter Kennwort-String.

[-x] <opCodeExt>
: Opcode-Erweiterung für die zu verschlüsselnden ConfigSpace-Daten.

[-p] <password>
Kennwort für die angegebene Objekt-ID.
Standard: 1452 (ConfBMCAcctUserPassword)

Unterstützte Werte:

1273 - ConfAlarmEmailSMTPAuthPassword

[-p] <password>
Kennwort für die angegebene Objekt-ID.
Standard: 1452 (ConfBMCAcctUserPassword)

Unterstützte Werte:

1452 - ConfBMCAcctUserPassword

1273 - ConfAlarmEmailSMTPAuthPassword

197A - ConfLdapiRMCgroupsUserPasswd

1980 - ConfBMCLicenseKey

iRMC_PWD Kommandozeilenausgabe-Optionen

[-b]
Erstellt die Ergebnisdatei als WinSCU BATCH-Datei.

[-f] <Ergebnisdatei>
Festlegen des Ergebnisdateinamens.
Standard: *iRMC_pwd.txt*
Standard im Batch-Modus: *iRMC_pwd.pre*

Beispiel

Sie möchten eine *.pre*-Datei erstellen, mit der der Benutzername auf `admin` und das Kennwort auf `SecretPassword` für den (bestehenden) Benutzer mit der oid `2` festgelegt/geändert wird.

Geben Sie dazu das folgende Kommando ein:

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
```

iRMC_PWD erstellt die *.pre*-Datei mit den in figure 226 on page 445 gezeigten Inhalten.

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b


<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CMDSEQ>
<!-- "ConfBMCAcctUserName" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1451" OI="2" Type="SET">
  <DATA Type="xsd::string">admin</DATA>
  <STATUS>0</STATUS>
</CMD>
<!-- "ConfBMCAcctUserPassword" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1452" OI="2" Type="SET">
  <DATA Type="xsd::string"
Encrypted="1">N2BZd3oLHAgc11pnHCAV9P/ItwRue4qBB3IU7Xsh</DATA>
  <STATUS>0</STATUS>
</CMD>
</CMDSEQ>
```

Figure 226: Inhalte der generierten .pre-Datei